Secure Switching

ALSO Tech-Workshop

24.10.2018

Jonas Walker, Systems Engineer, jwalker@fortinet.com, +41797259413

Agenda

Simplified Management

Scalable Topologies

Integrated Security

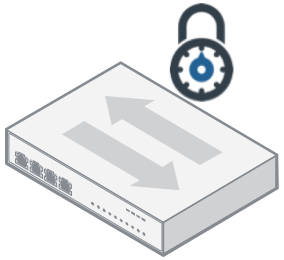
Live Demo ☺

SUMMARY

ZERO-TOUCH PROVISIONING

- Easy deployment in high scale
- No login to the switches
- Auto Discovery of Switches

SECURE AND CENTRALIZED CONFIGURATION MANAGEMENT

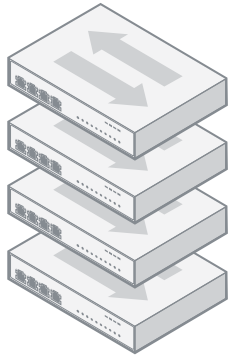


- FortiGate is Single Point of Management
- Centralized VLAN and Features provisioning

SECURITY FABRIC INTEGRATION

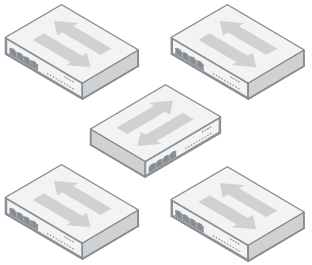
- Device Discovery
- Centralized Authentication
- Host Quarantine
- Dynamic VLAN Assignment
- Logging

FORTISWITCH STACK



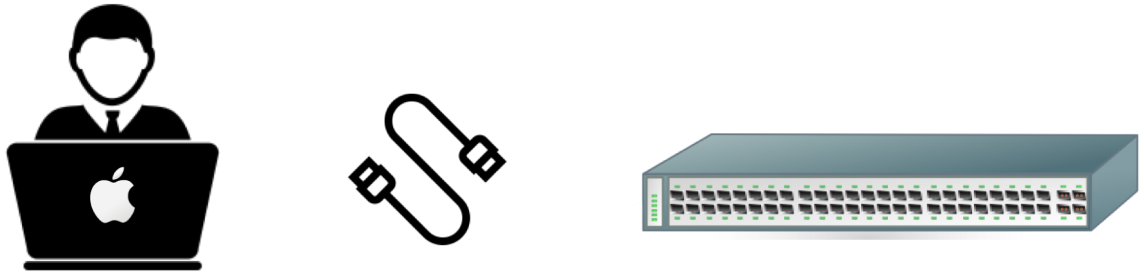
- Stack of FortiSwitches Controlled by FortiGate (Single or HA-Pair)
- MCLAG for loop-free link and switch level redundancy

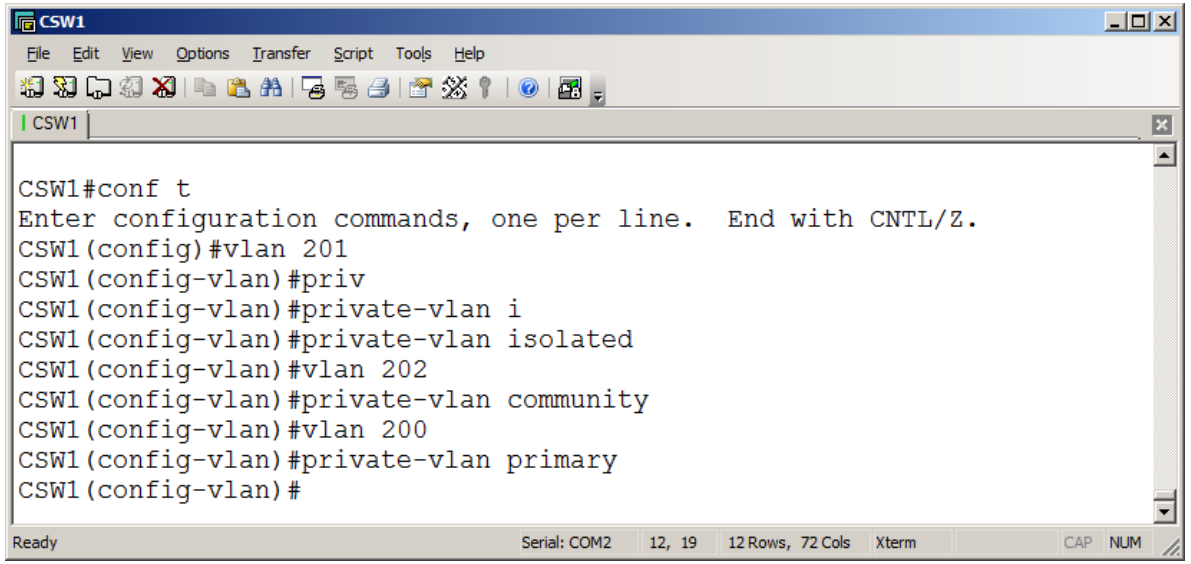
MODEL RANGE

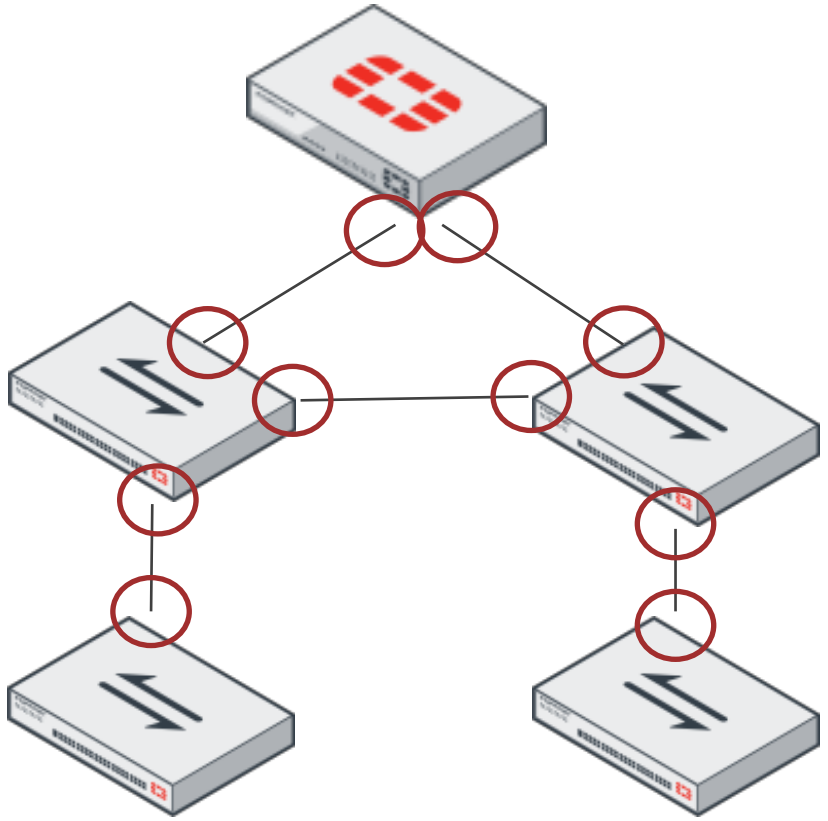


- Range of FortiSwitch and FortiGate Models for
  - Retail
  - SMB
  - Enterprise
  - Datacenter

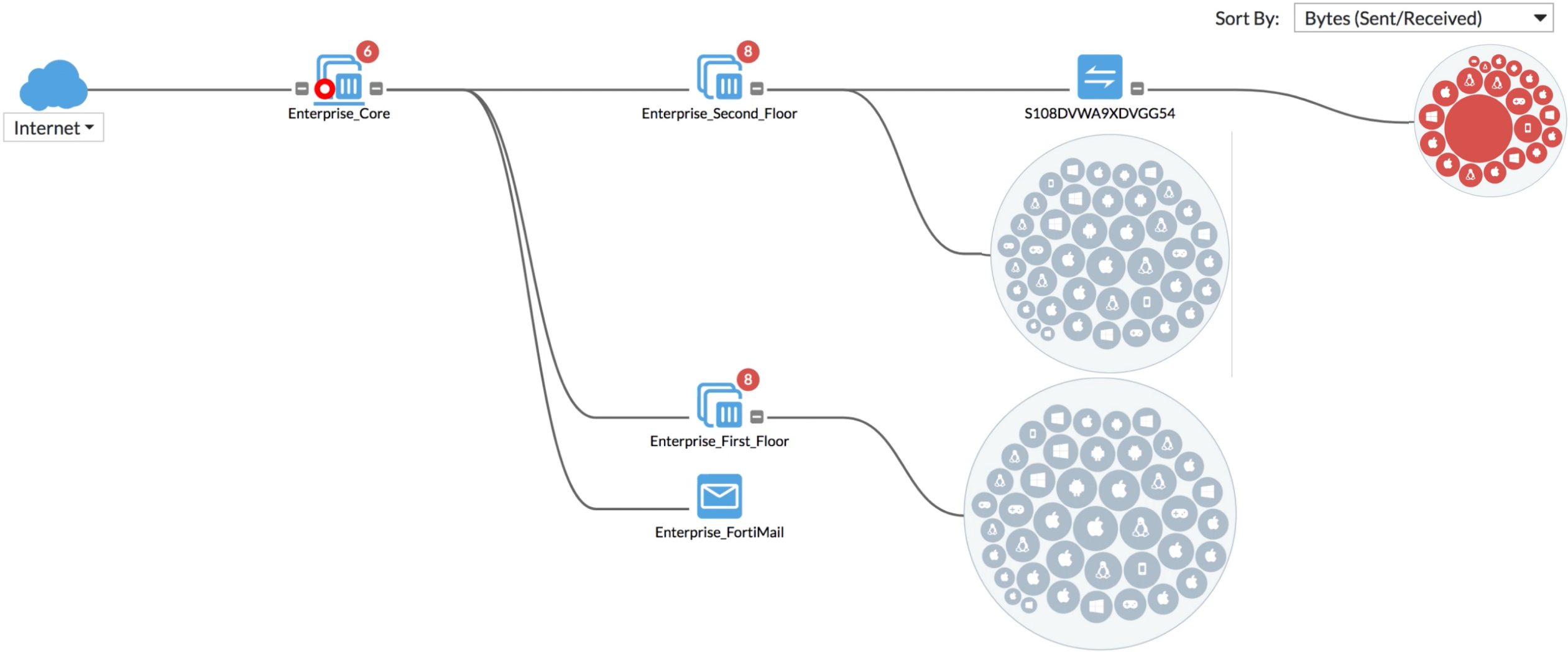
Simplified Management

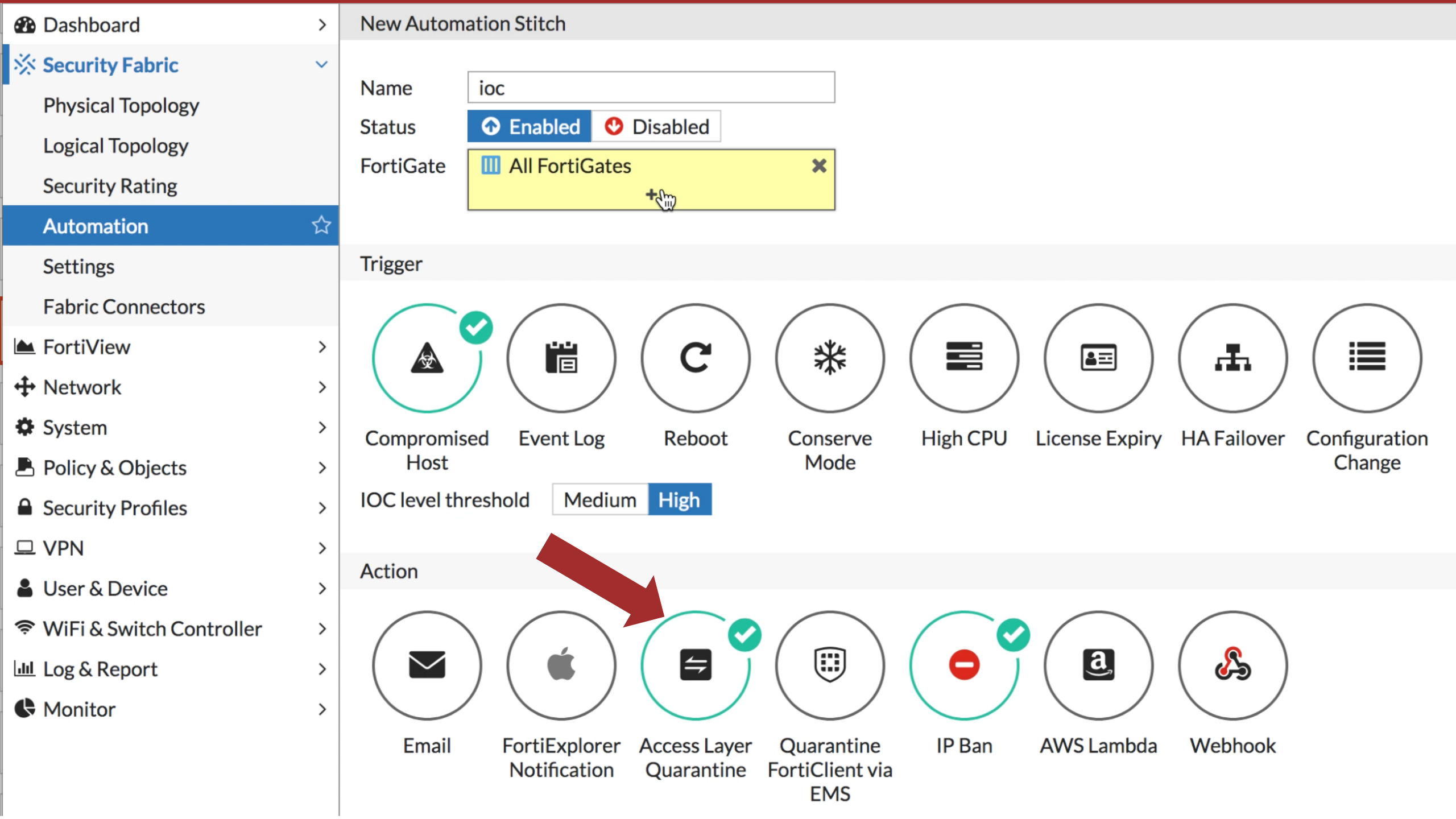


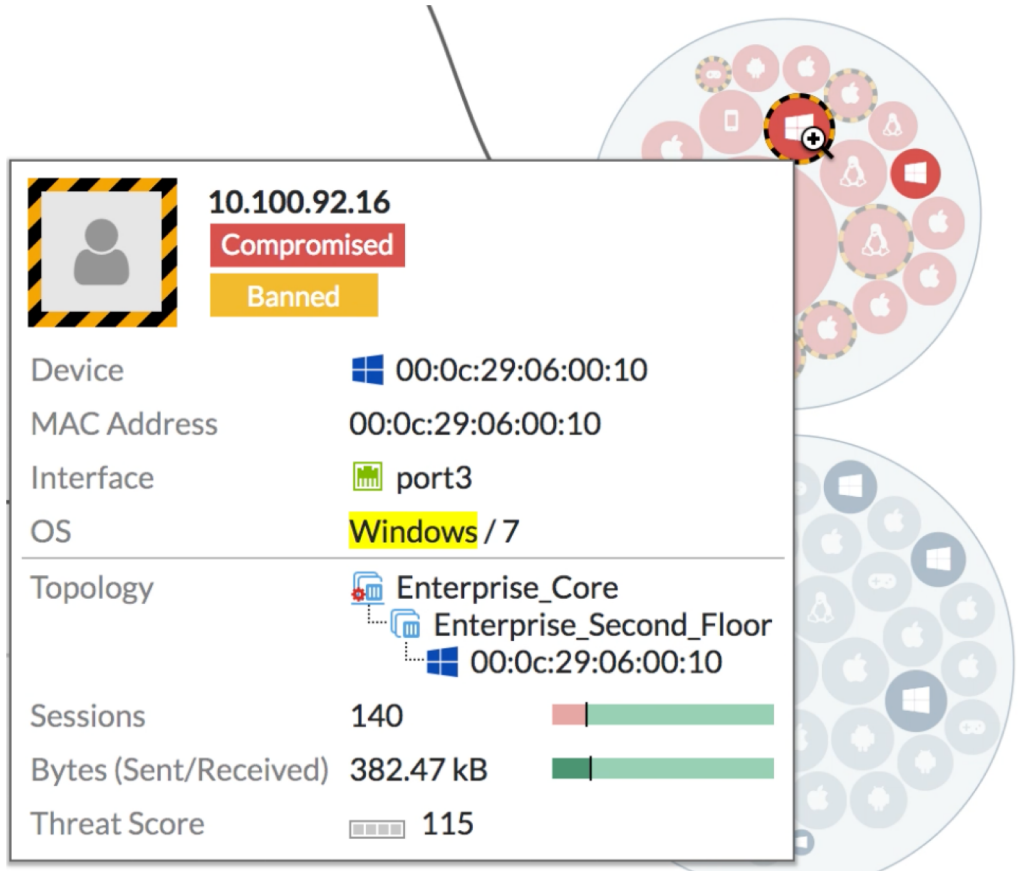





RED5
the ultimate gadget shop
thecore


Sort By:
Bytes (Sent/Received)
Internet
6
Enterprise_Core
8
Enterprise_Second_Floor
S108DVWA9XDVGG54
8
Enterprise_First_Floor
Enterprise_FortiMail


Dashboard
Security Fabric
Physical Topology
Logical Topology
Security Rating
Automation
Settings
Fabric Connectors
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor
New Automation Stitch
Name
ioc
Status
Enabled
Disabled
FortiGate
All FortiGates
Trigger
Compromised Host
Event Log
Reboot
Conserve Mode
High CPU
License Expiry
HA Failover
Configuration Change
IOC level threshold
Medium
High
Action
Email
FortiExplorer Notification
Access Layer Quarantine
Quarantine FortiClient via EMS
IP Ban
AWS Lambda
Webhook


10.100.92.16
Compromised
Banned
Device
00:0c:29:06:00:10
MAC Address
00:0c:29:06:00:10
Interface
port3
OS
Windows / 7
Topology
Enterprise_Core
Enterprise_Second_Floor
00:0c:29:06:00:10
Sessions
140
Bytes (Sent/Received)
382.47 kB
Threat Score
115

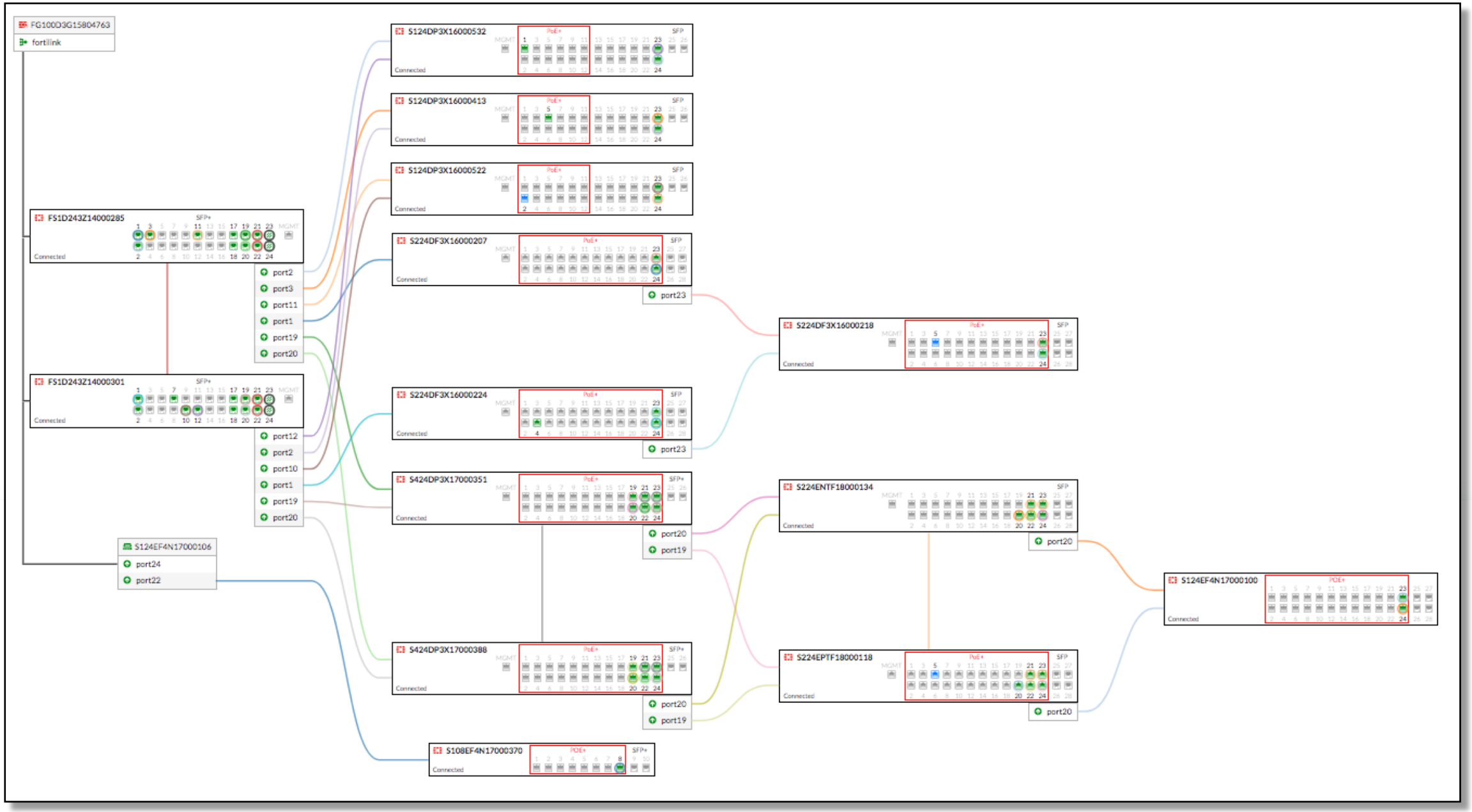
FortiLink

FOS 5.4.3 and later – Max number of FSW per FGT

FGT Model	Max number of FSW (hard limit)
up to FG-98D / VM01	8 → 16 (E and later suffix 6.2.0, save FGT-91E)
FG-100-E to FG-280D / VM02	24 → 32 (E and later suffix 6.2.0)
FG-300D to FG-500D/E	48
FG-600D to FG-900D / VM04	64
FG-1000D to FG-2xxxE	128
FG-3xxx and above / VM08	300

Fortilink Port Assignment

FortiSwitch	Default Ports for Fortilink * any port can be used if manually configured
FS-108D-POE	9 and 10
FS-108E, FS-108E-POE, FS-108E-FPOE	7, 8, 9 and 10
FSR-112D-POE	5, 6, 7, 8, 9, 10, 11 and 12
FS-224D-POE	21, 22, 23 and 24
FS-124D, FS-124D-POE	23, 24, 25 and 26
FS-124E, FS-124E-POE, FS-124E-FPOE, FS-224D-FPOE, FS-224E, FS-224E-POE	21, 22, 23, 24, 25, 26, 27 and 28
FS-248D, FS-248D-FPOE, FS-248E-POE, FS-248E-FPOE FS-448D, FS-448D-FPOE, FS-448D-POE	45, 46, 47, 48, 49, 50, 51 and 52
FS-248D-POE	47, 48, 49 and 50
FS-424D, FS-424D-FPOE, FS-424D-POE	23, 24, 25 and 26
FS-524D, FS-524D-FPOE	21, 22, 23, 24, 25, 26, 27, 28, 29 and 30
FS-548D-FPOE, FS-548D	45, 46, 47, 48, 49, 50, 51, 52, 53 and 54
FS-1024D, FS-1048D, FS-3032D, FS-1048E	all ports


FG100D3G15804763
fortilink
FS1D243Z14000285
Connected
port2
port3
port11
port1
port19
port20
FS1D243Z14000301
Connected
port12
port2
port10
port1
port19
port20
S124EF4N17000106
port24
port22
S124DP3X16000532
Connected
S124DP3X16000413
Connected
S124DP3X16000522
Connected
S224DF3X16000207
Connected
port23
S224DF3X16000224
Connected
port23
S424DP3X17000351
Connected
port20
port19
S424DP3X17000388
Connected
port20
port19
S108EF4N17000370
Connected
S224DF3X16000218
Connected
S224ENTF18000134
Connected
port20
S224EPTF18000118
Connected
port20
S124EF4N17000100
Connected

What's running on FortiLink?

- FortiLink Heartbeat
- LLDP → FSW discovery
- CAPWAP → configuration commands, software upgrade
- NTP → time sync with FGT
- HTTPS → config and diag commands via REST API

FortiSwitch Auto Inter-switch link

- ISL are autoconfigured after FSW is controlled by FGT

```
S224DF3X16000224 # show switch physical-port port24
config switch physical-port
    edit "port24"
        set lldp-profile "default-auto-isl"
        set speed auto
    next
end
S224DF3X16000224 # show switch lldp profile default-auto-isl
config switch lldp profile
    edit "default-auto-isl"
        set auto-isl enable
    next
end
S224DF3X16000224 # config switch physical-port
S224DF3X16000224 (physical-port) # edit port24
S224DF3X16000224 (port24) # get
name                 : port24
cdp-status           : disable
description          : (null)
dmi-status           : global
flow-control         : rx
l2-learning          : enabled
link-status          : down
lldp-profile         : default-auto-isl
lldp-status          : tx-rx
max-frame-size       : 9216
poe-pre-standard-detection: enable
poe-status           : enable
port-index           : 24
speed                : auto
status               : up
```

FortiSwitch Auto Inter-switch link

- ISL are autoconfigured as trunks

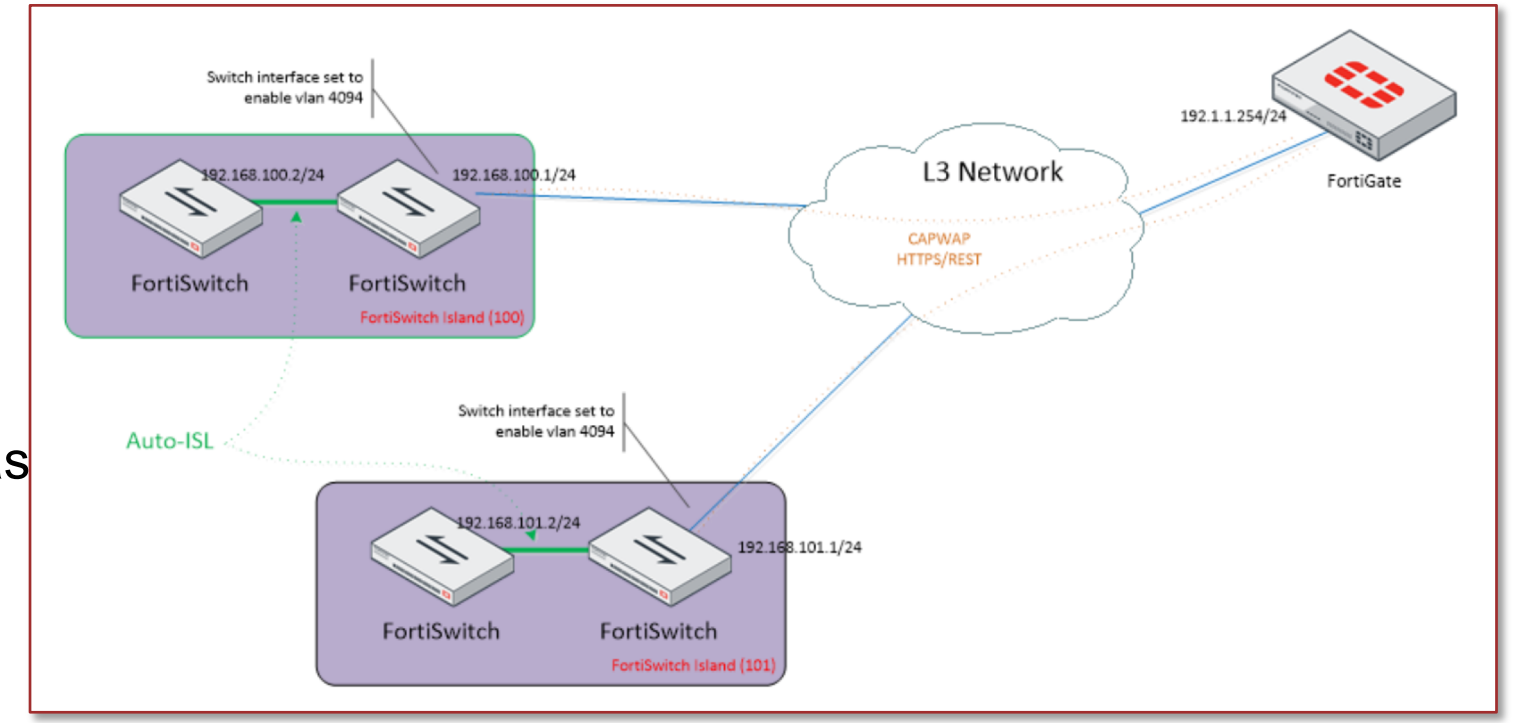
```
FS108D3W16000186 # config switch interface
FS108D3W16000186 (interface) # edit 08D3W16000183-0
FS108D3W16000186 (08D3W16000183-0) # show
config switch interface
    edit "08D3W16000183-0"
        set native-vlan 4094
        set allowed-vlans 1-4095
        set snmp-index 13
    next
end
FS108D3W16000186 (08D3W16000183-0) # get
name                : 08D3W16000183-0
type                : trunk
native-vlan         : 4094
allowed-vlans       : 1-4095
untagged-vlans      :
stp-state           : enabled
stp-loop-protection : disabled
edge-port           : disabled
dot1x               : disable
mab                 : disable
fortilink-intf-mode : disable
dynamic-fortilink-mode: disable
snmp-index          : 13
```

FortiLink over L3

FortiLink over L3

FSW is controlled by FGT From Anywhere in the World!

- Available on FSWOS 3.6.4 GA and FOS 6.0.0 GA
- Allows to manage FSWs with Fortilink over L3 networks. FSW Islands (FSI)
- Limitations:
  - » Same number of FSW per FGT as with regular Fortilink
  - » Only management and configuration on Fortilink
  - » Data traffic stays in the FSW Islands – **no tunneling to FGT**

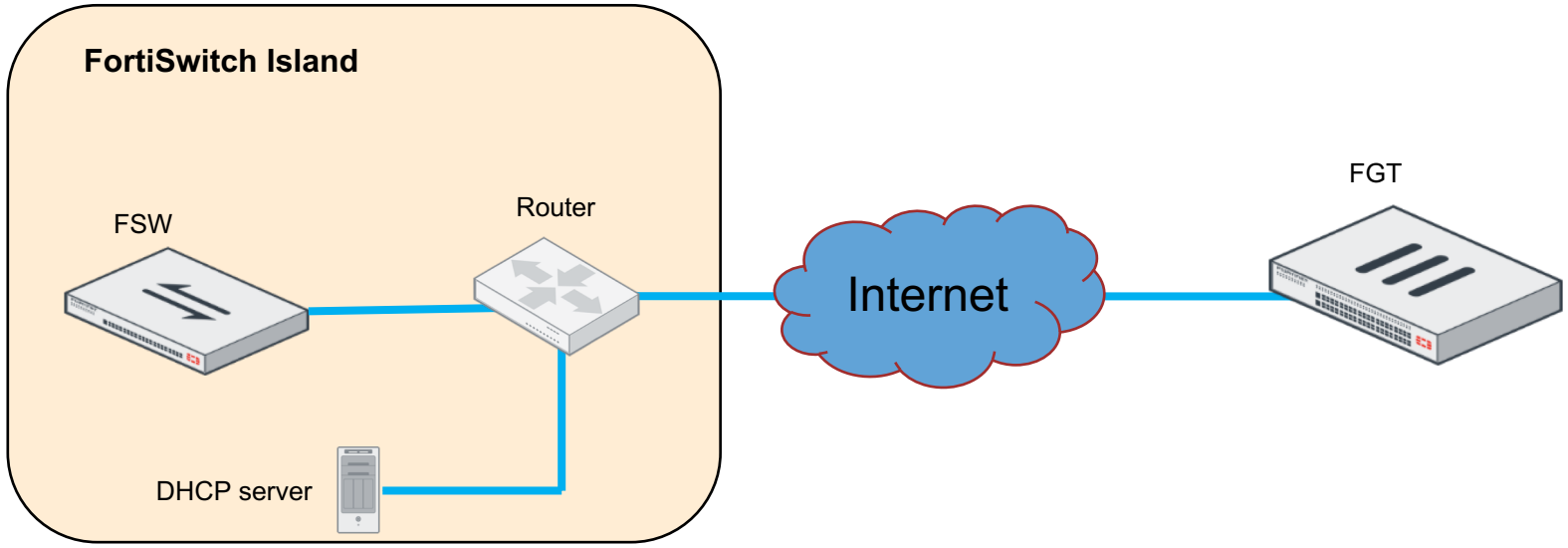


Feature Support

Feature	FortiLink (direct L2 connection)	FortiLink over L3
Centralized Configuration	✓	✓
Centralized Firmware Management	✓	✓
LAG support for FortiLink Connection	✓	✓
802.1x Authentication (Port-based, MAC-based, MAB)	✓	✓
Host Quarantine on Switch Port	✓	✓
Device Detection	✓	Prototype
Support FortiLink FortiGate in HA Cluster	✓	✓
Active-Active Split MCLAG from FortiGate to FortiSwitch	✓	
Access VLAN	✓	
DHCP Server on VLAN defined on FGT	✓	

FortiLink over L3 – Scenario

FSW Reach Switch Controller over L3 Network Routed on Central FGT



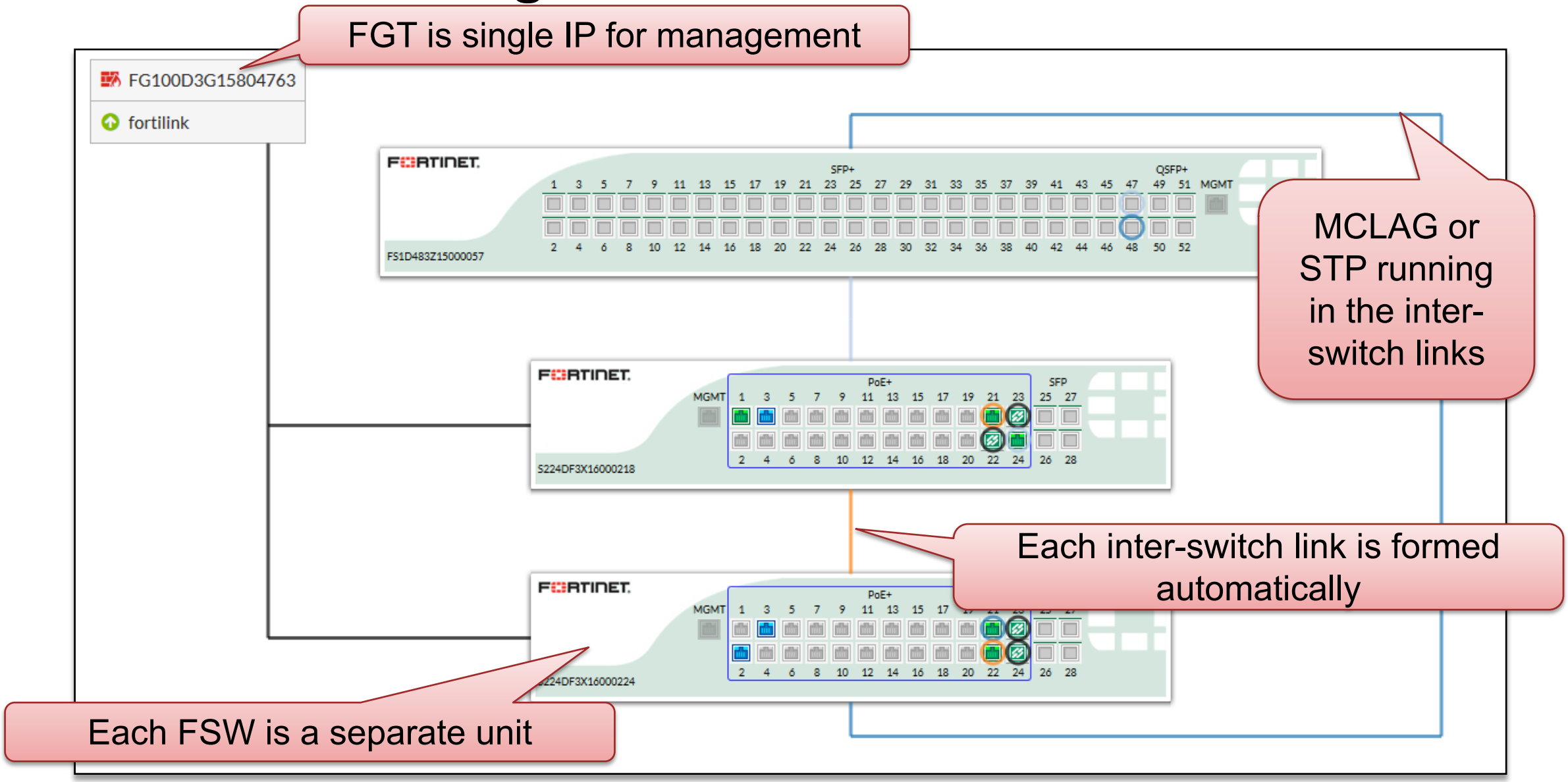
DESIGN ALTERNATIVES

FortiLink Stacking

High Port Density with Ease of Management

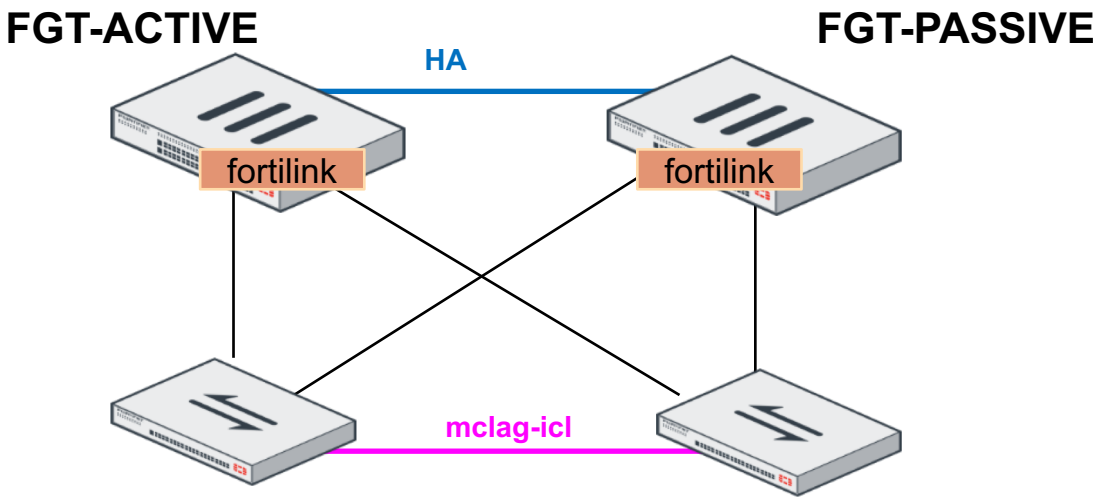
- Single IP for Management
  - FortiGate is the switch controller
- Wide Range of solutions
  - From SMB/Retail to Data Center
    - 8 ports with single FortiSwitch to
    - more than a thousand ports with multiple FortiSwitches
  - Any combination of Gig or 10G Switches
  - Multiple topologies supported
- Collapsed layers
  - Physically 2 layers (FortiGate-Routing/Security and FortiSwitch-Switching)
  - Logically single layer

How does stacking work?



MCLAG

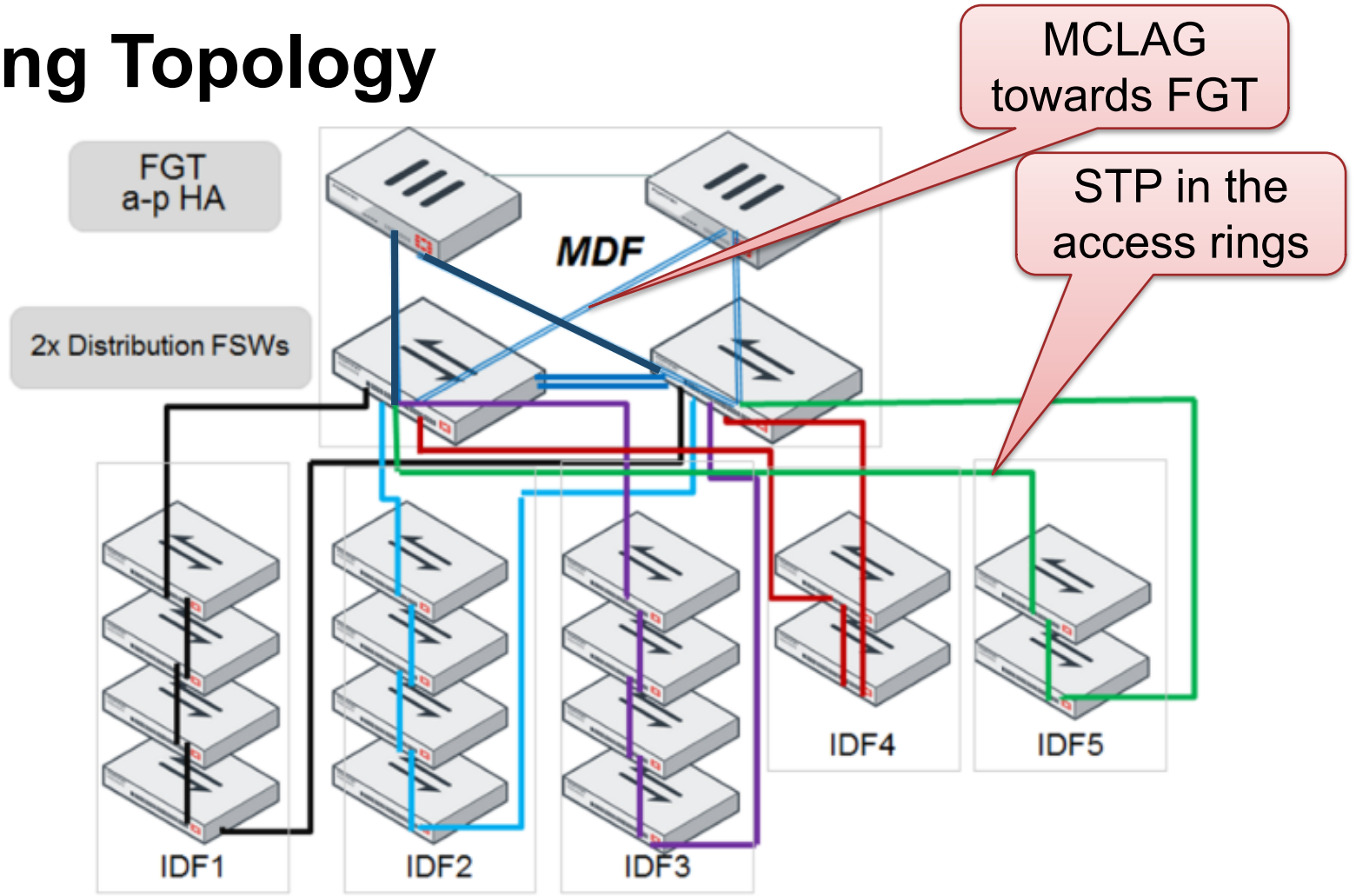
1st TIER MCLAG



MCLAG + RINGS

MCLAG + Access Ring Topology

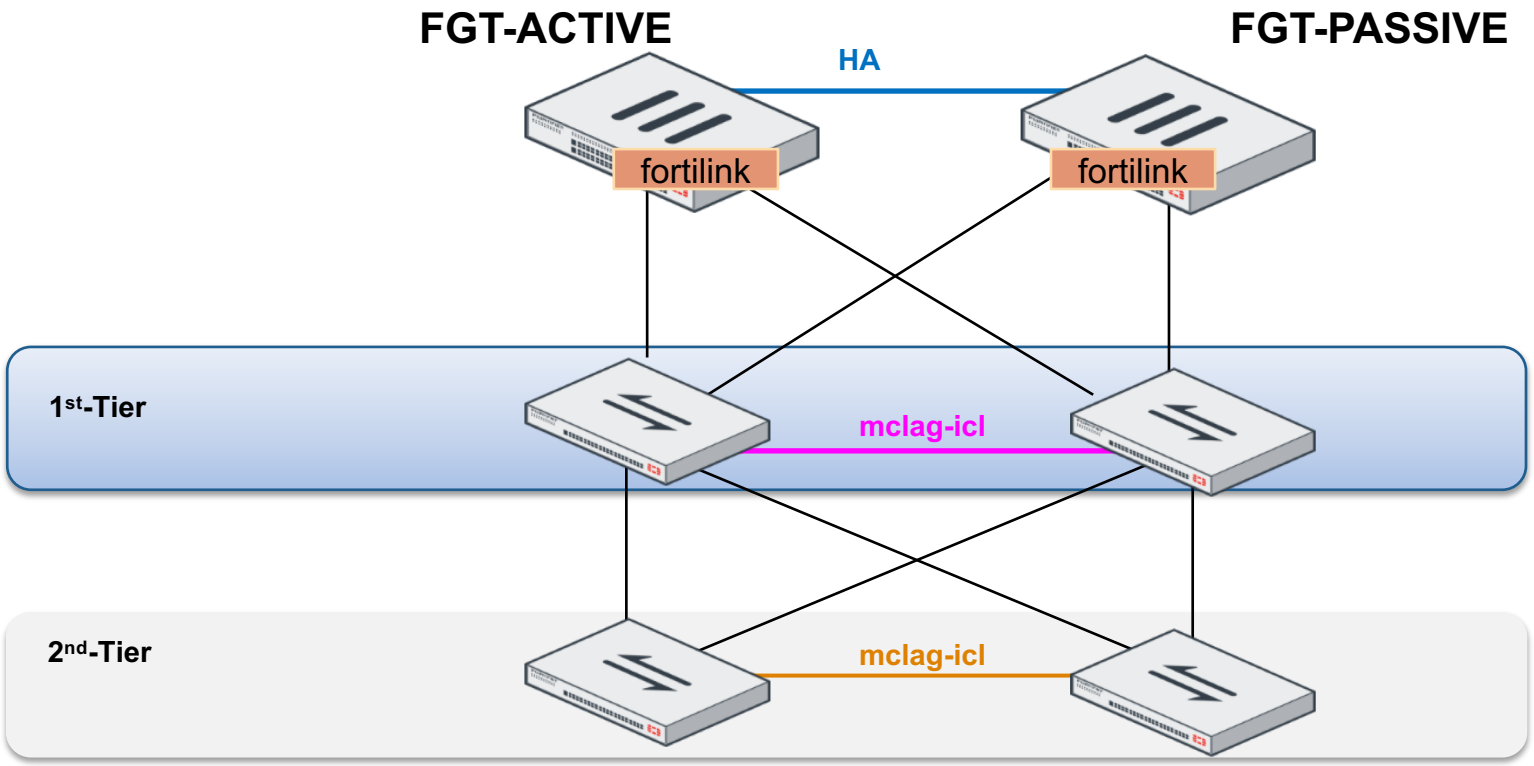
- Distribution FSW will implement MCLAG and MCLAG ICL
- Automatic STP configuration with the Access rings
- Both distribution FSWs will be seen as one STP entity, and both present same root MAC address and priority



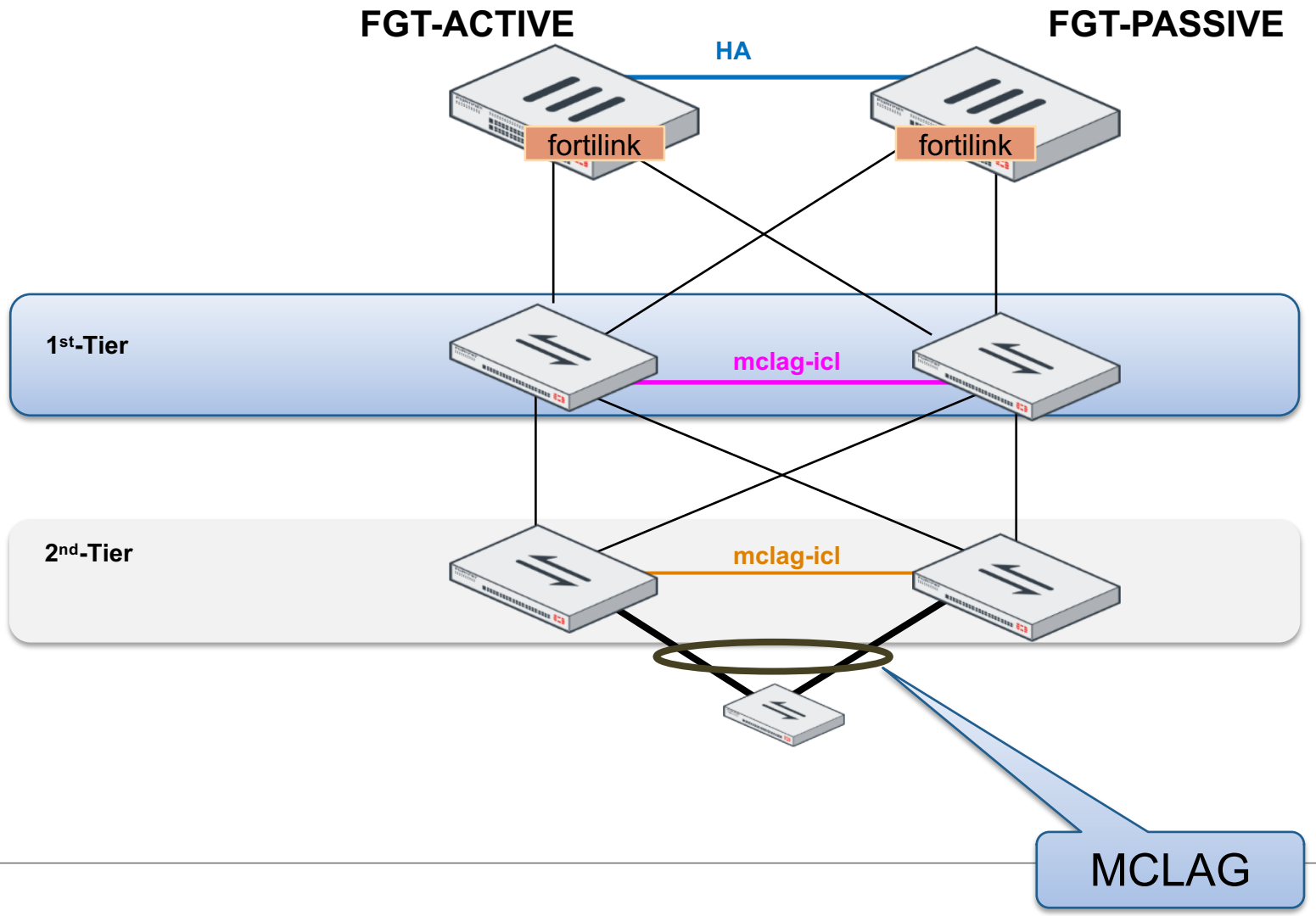
- Number of rings limited by the amount of ports on Distribution layer (max: 48)
- Number of switches in a ring limited by STP max hops (default: 20)

2nd TIER MCLAG

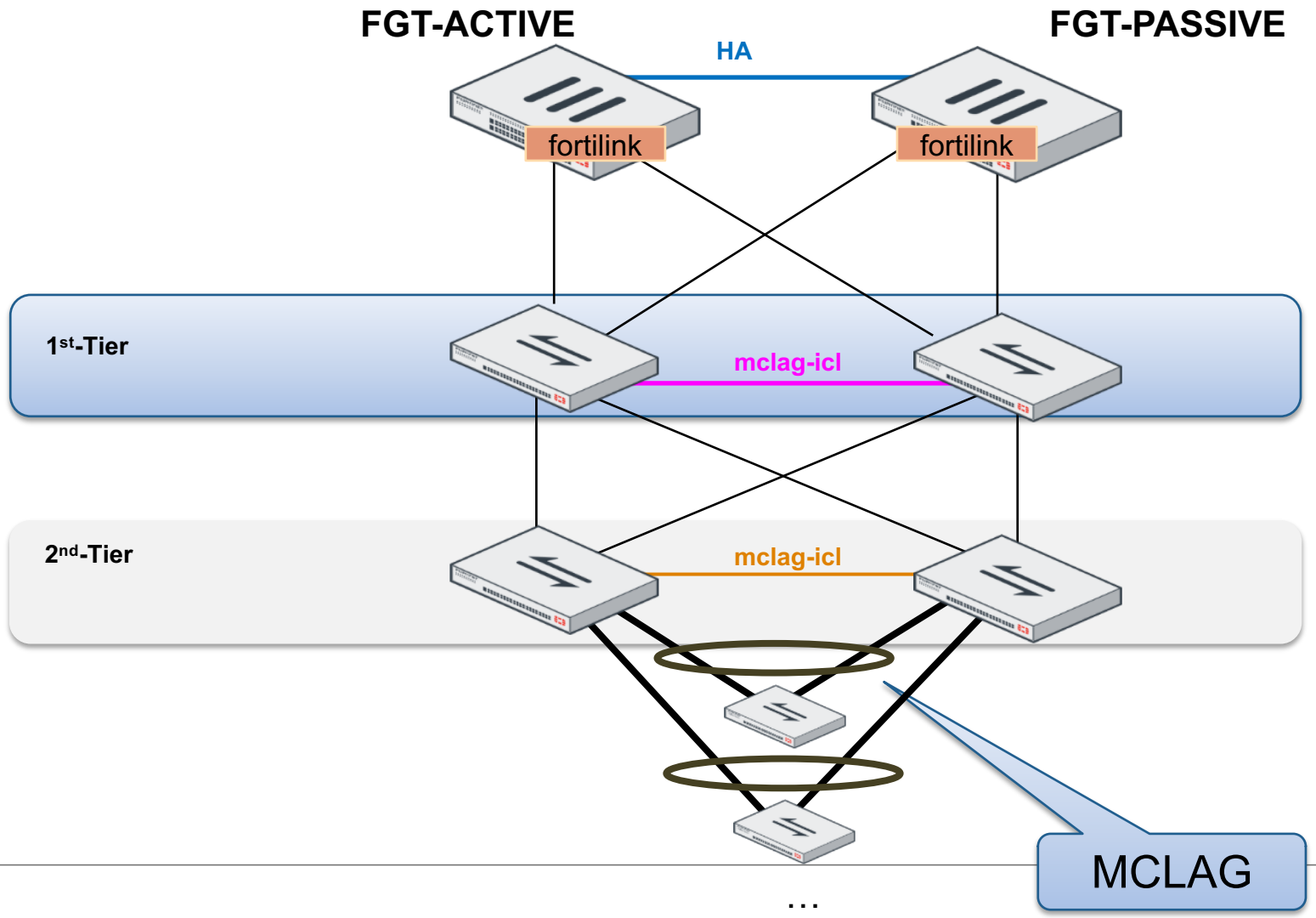
2nd TIER MCLAG



Dual-Homed Access Switches

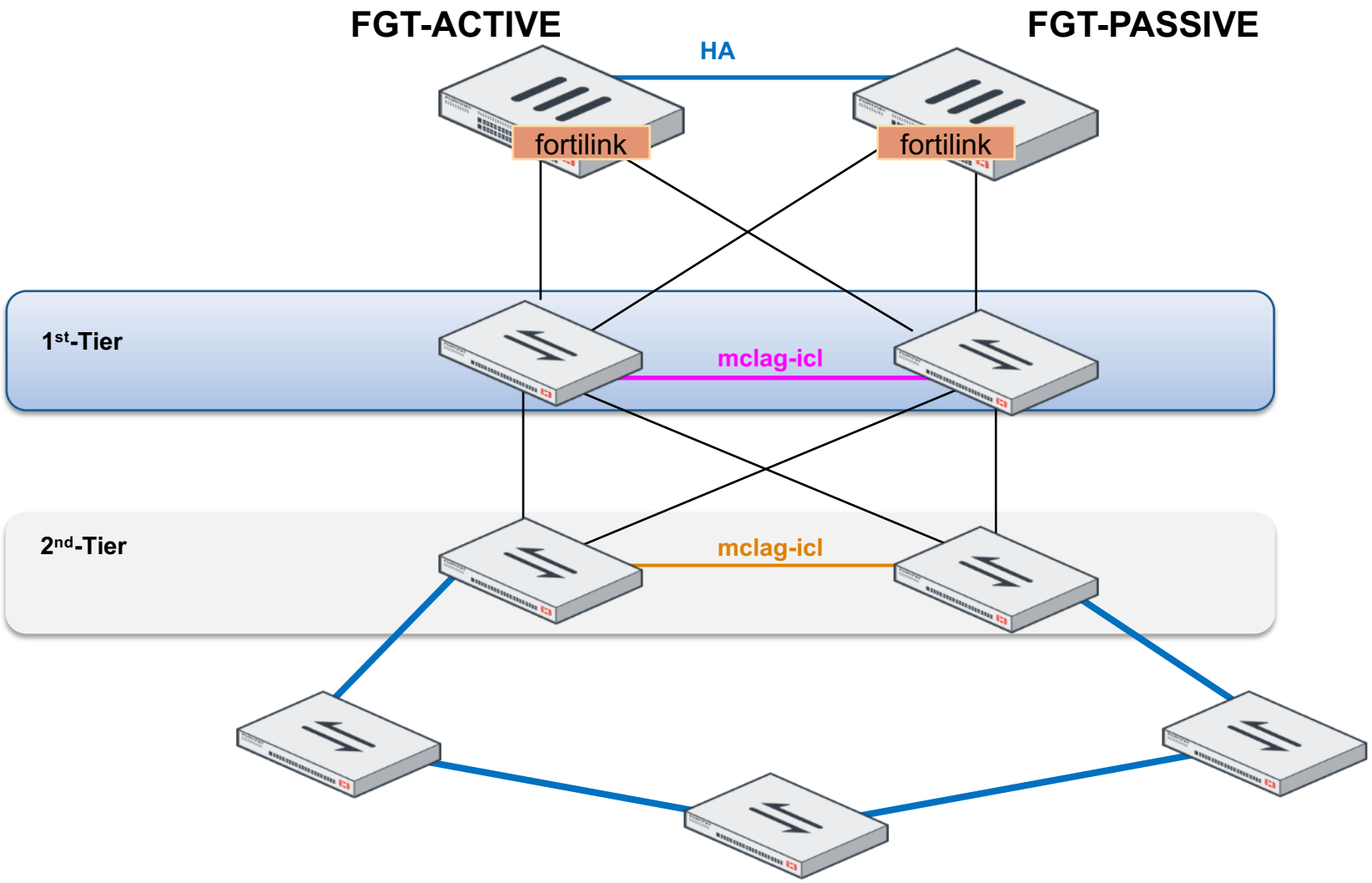


Dual-Homed Access Switches as complement to Stack

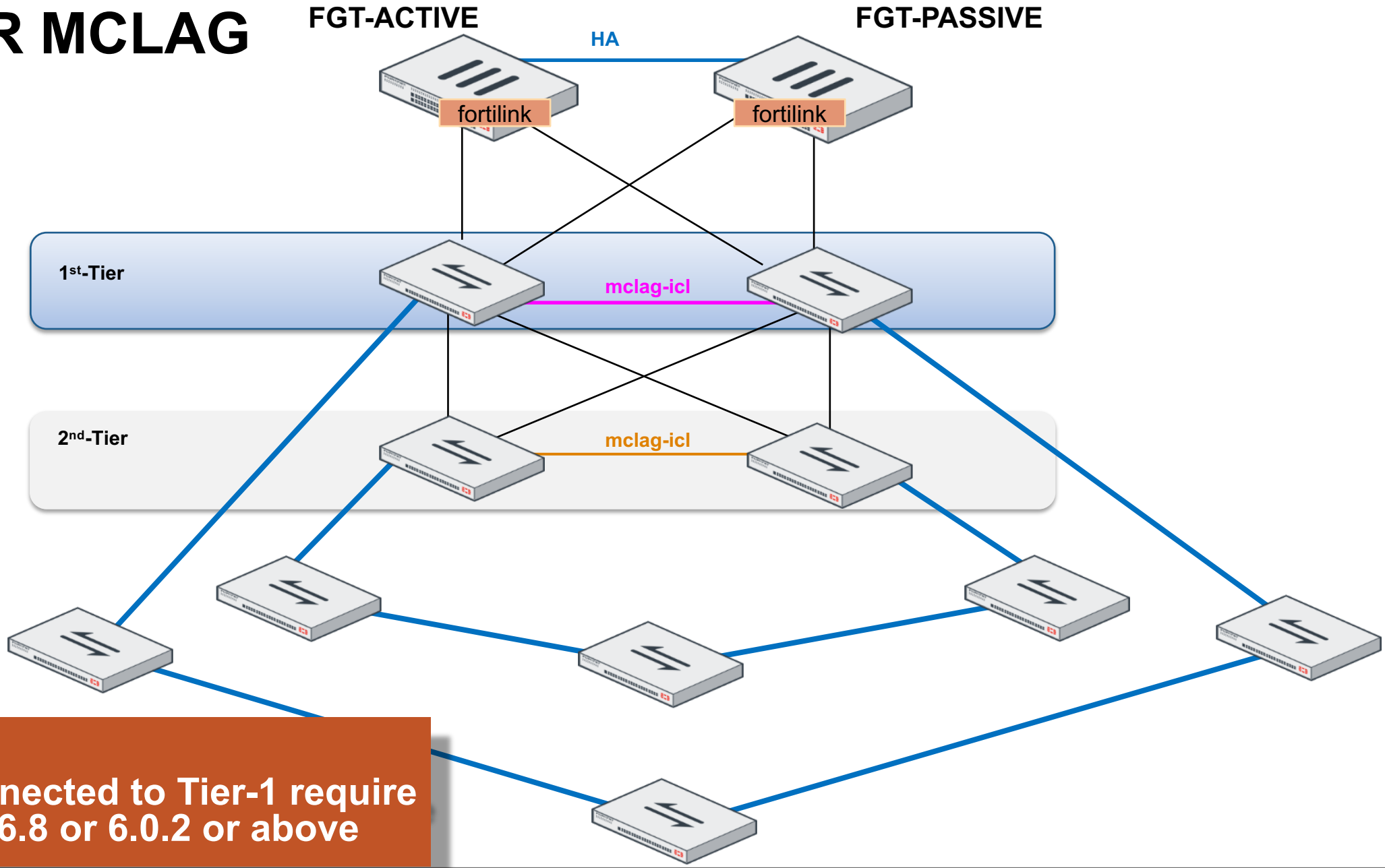


2nd TIER MCLAG + RINGS

2nd TIER MCLAG



2nd TIER MCLAG



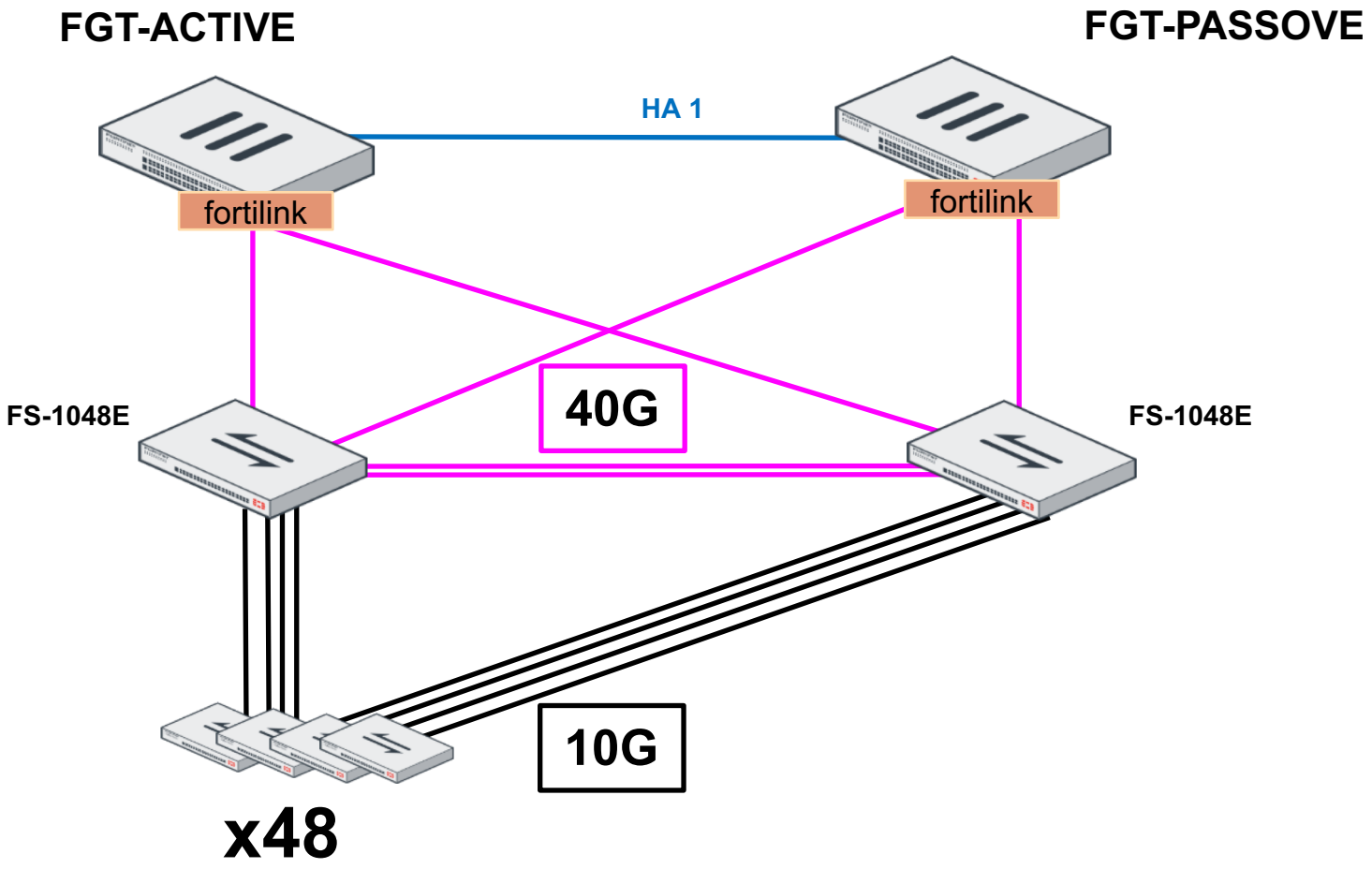
TIP

Rings connected to Tier-1 require FSWOS 3.6.8 or 6.0.2 or above

LARGE ENTERPRISE EXAMPLES

Large Scale Deployment

FortiLink

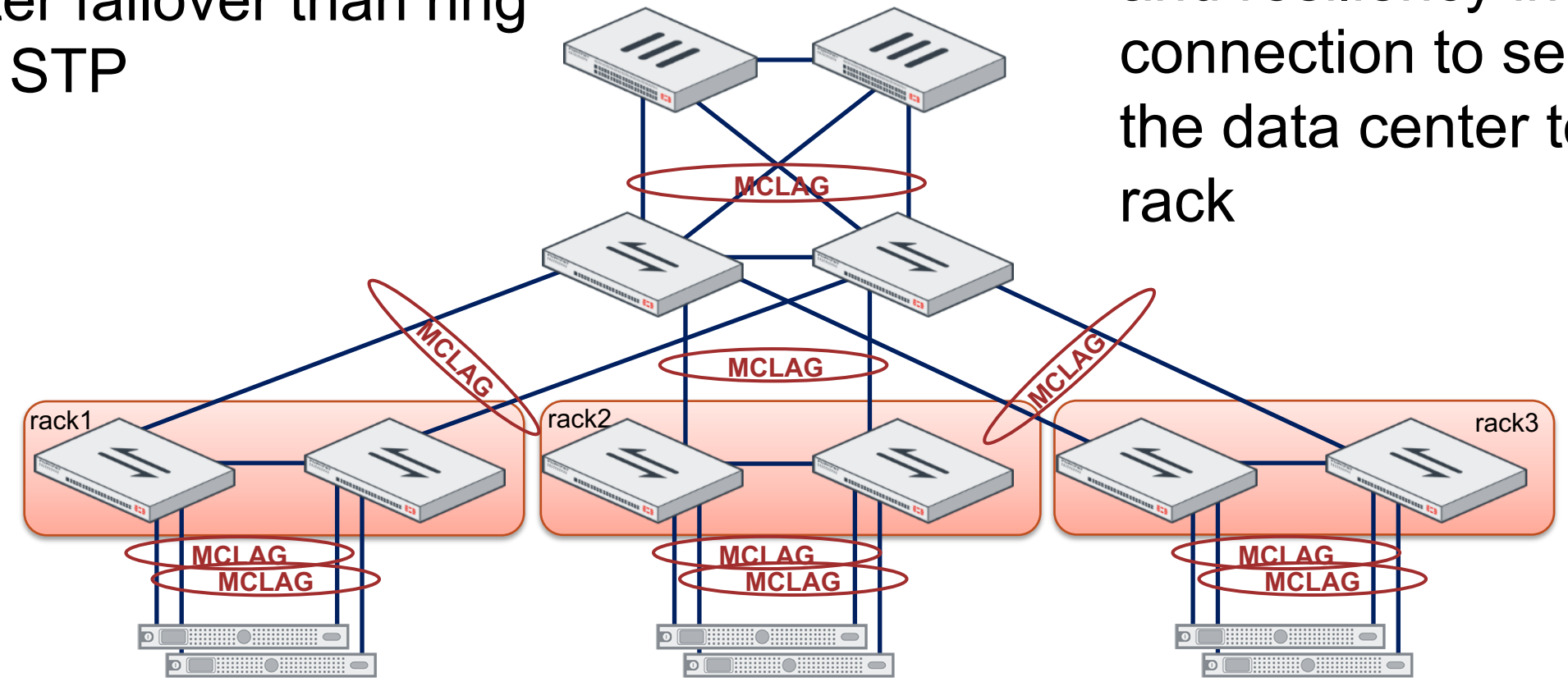


Total number of ports: 48 x 48 = 2304

Large Enterprise Deployment

MCLAG – Link and Switch Redundancy – Loop Free Topology

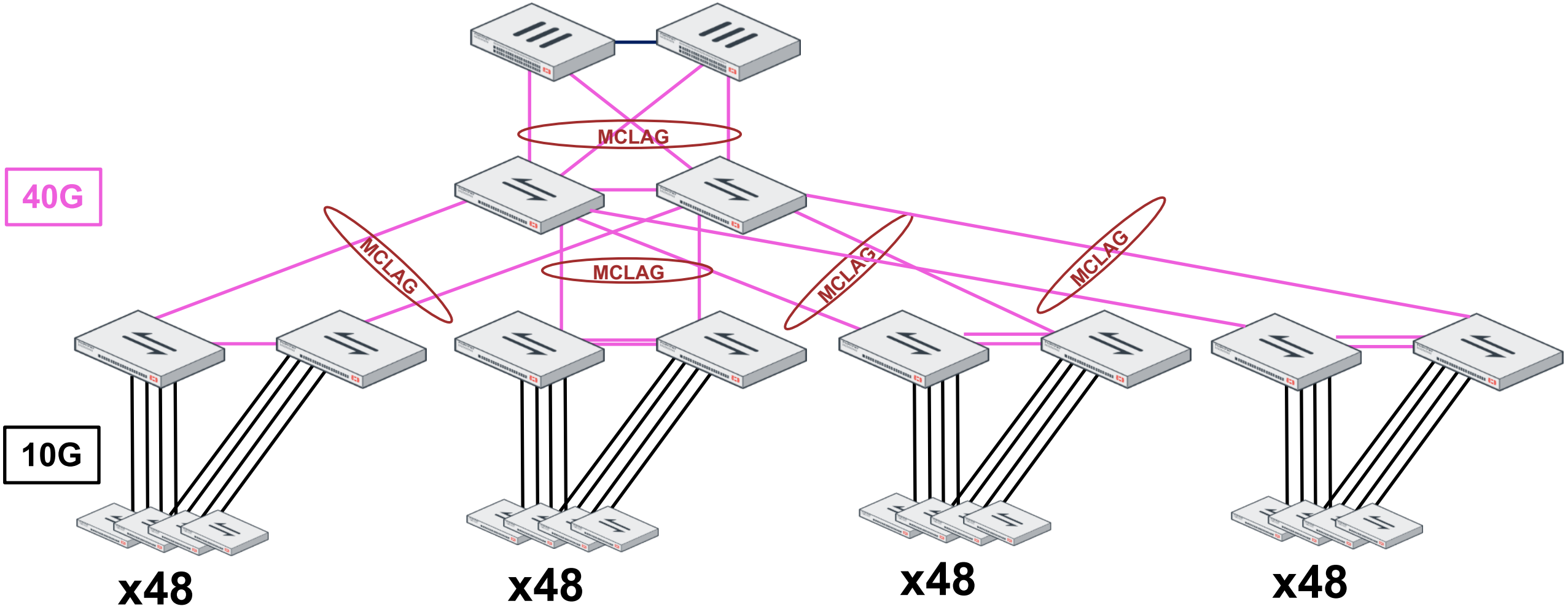
- More scalable design
- Faster failover than ring with STP



- Allows more bandwidth and resiliency in the connection to servers in the data center top of the rack

Even Larger Enterprise Deployment

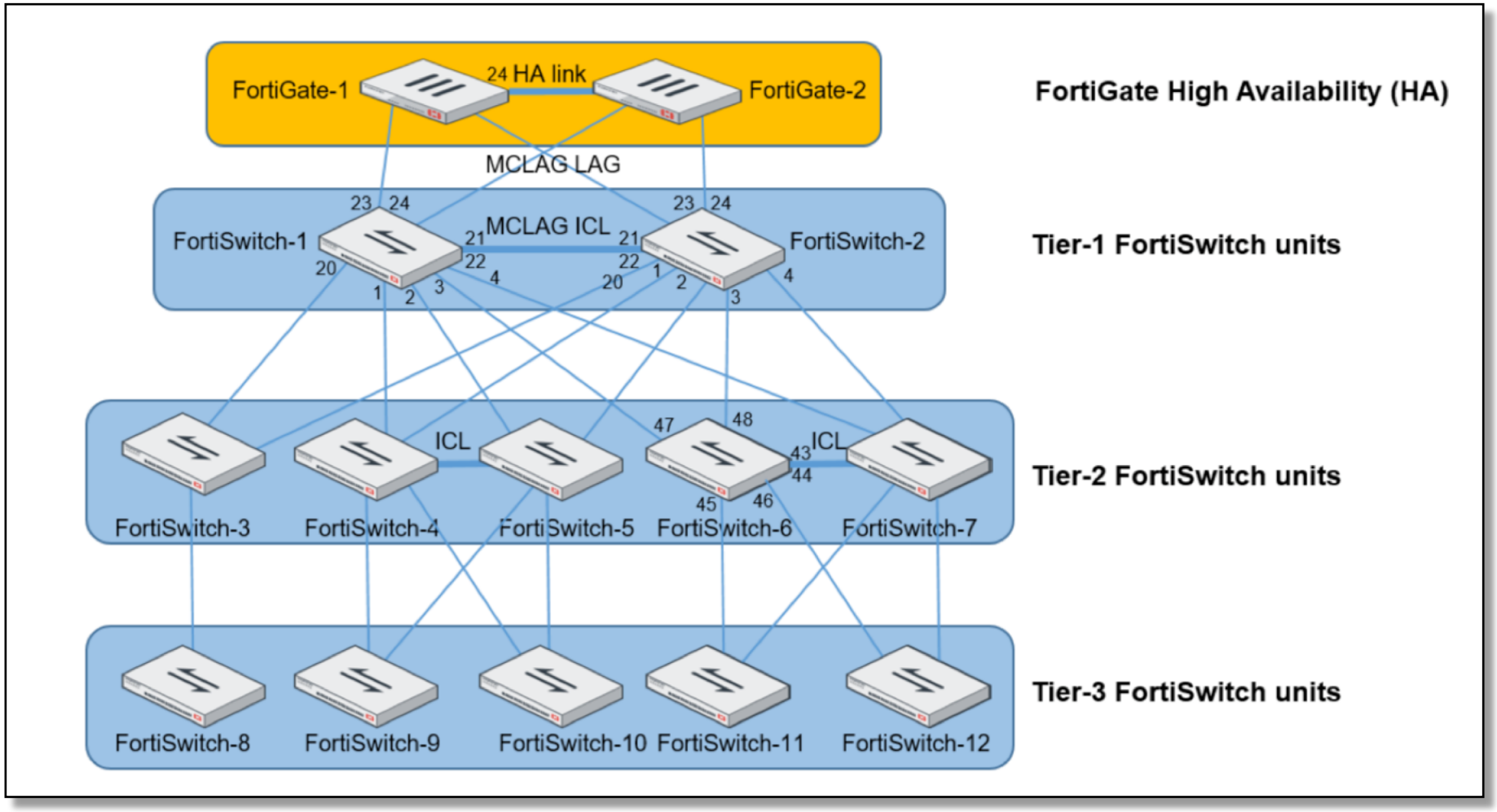
MCLAG – Link and Switch Redundancy – Loop Free Topology



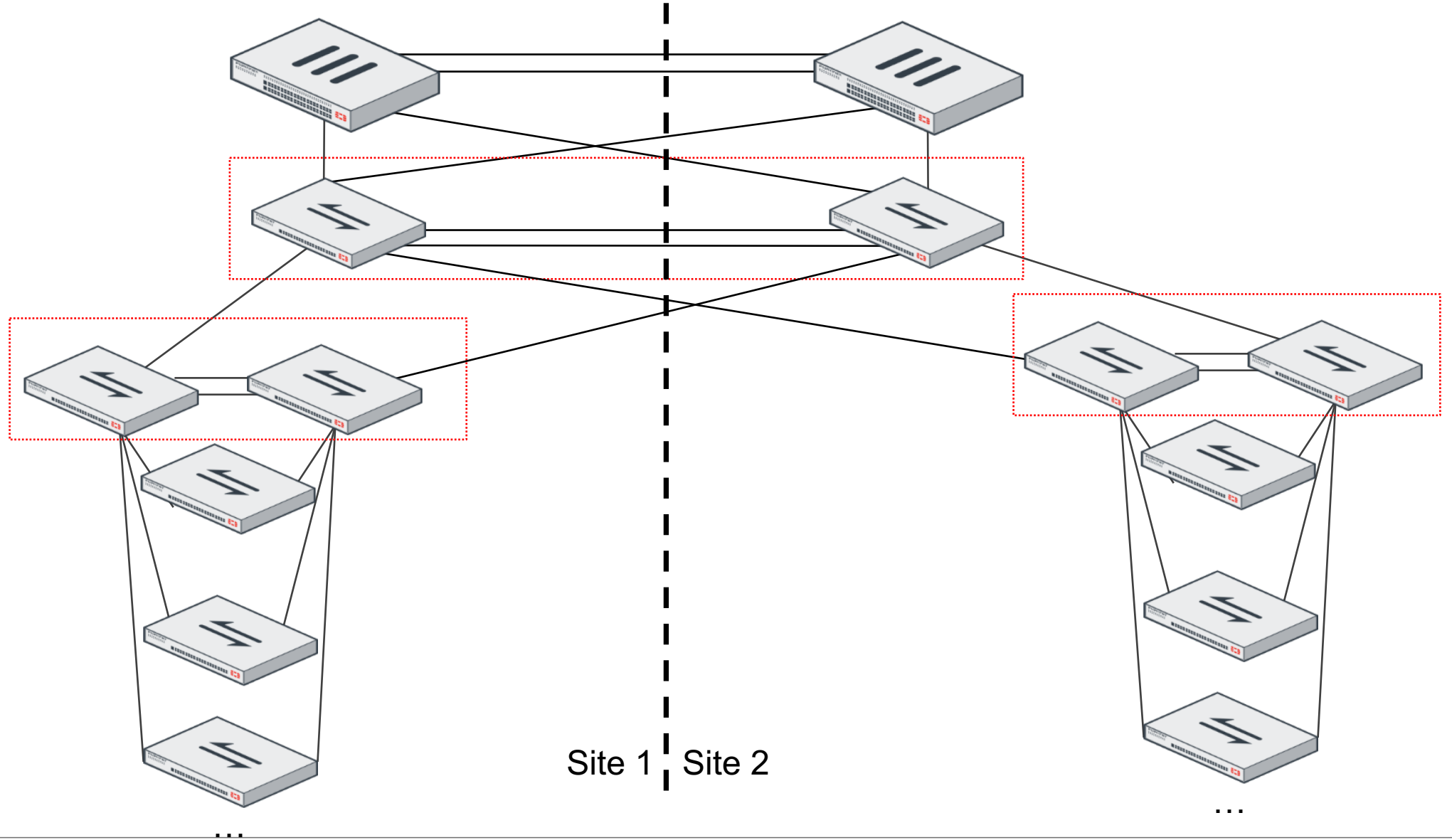
Total number of ports: 4x (48 x 48) = 9216

Large Scale Deployment

FortiLink

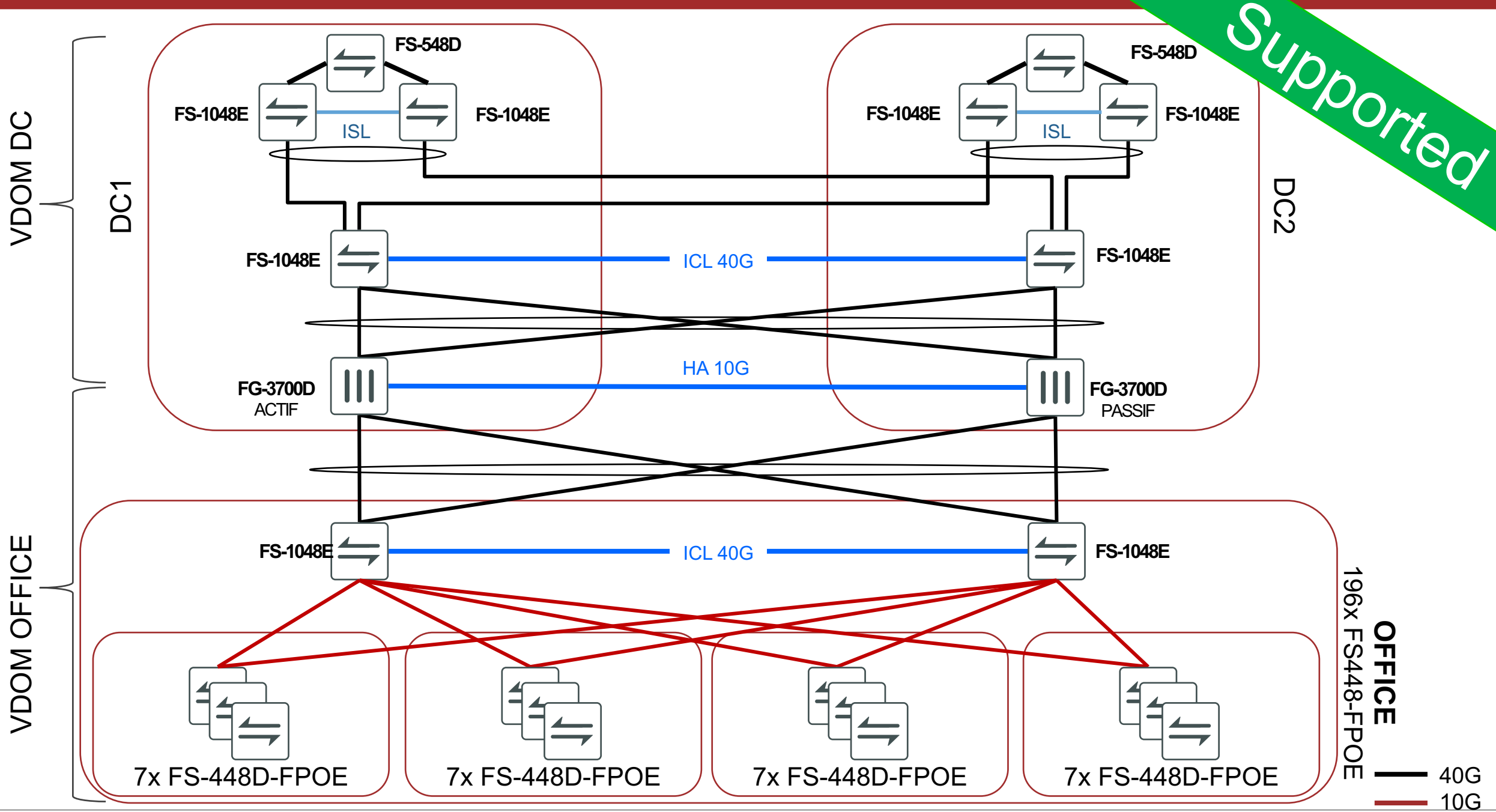


One L2 domain but 2 sites



GETTING CREATIVE?

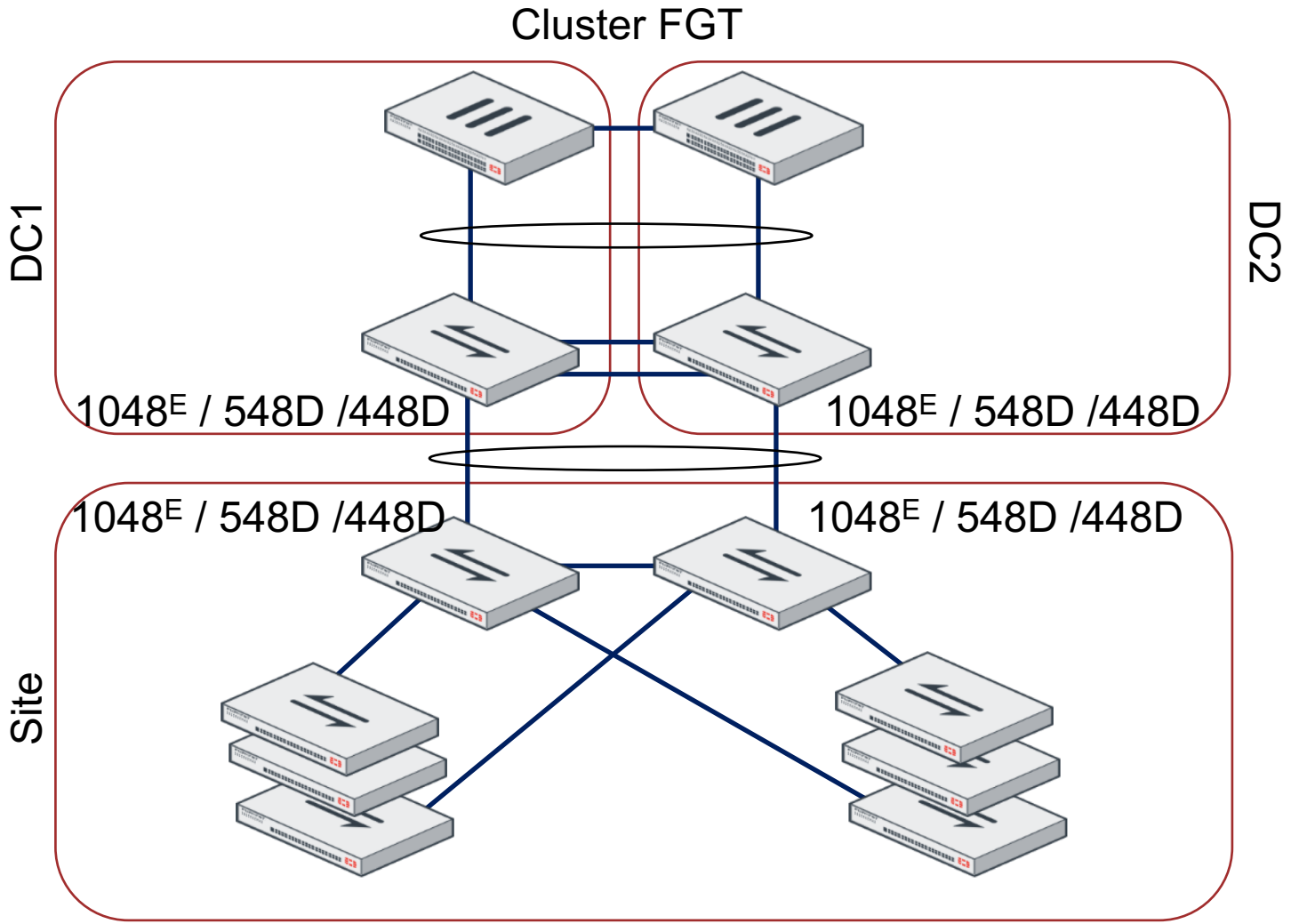
Will the following deployments be supported?


Supported
VDOM DC
DC1
DC2
FS-548D
FS-1048E
ISL
FS-1048E
FS-548D
FS-1048E
ISL
FS-1048E
FS-1048E
ICL 40G
FS-1048E
HA 10G
FG-3700D
ACTIF
FG-3700D
PASSIF
VDOM OFFICE
FS-1048E
ICL 40G
FS-1048E
7x FS-448D-FPOE
7x FS-448D-FPOE
7x FS-448D-FPOE
7x FS-448D-FPOE
OFFICE
196x FS448-FPOE
40G
10G

Design

Dual Home with FortiSwitch

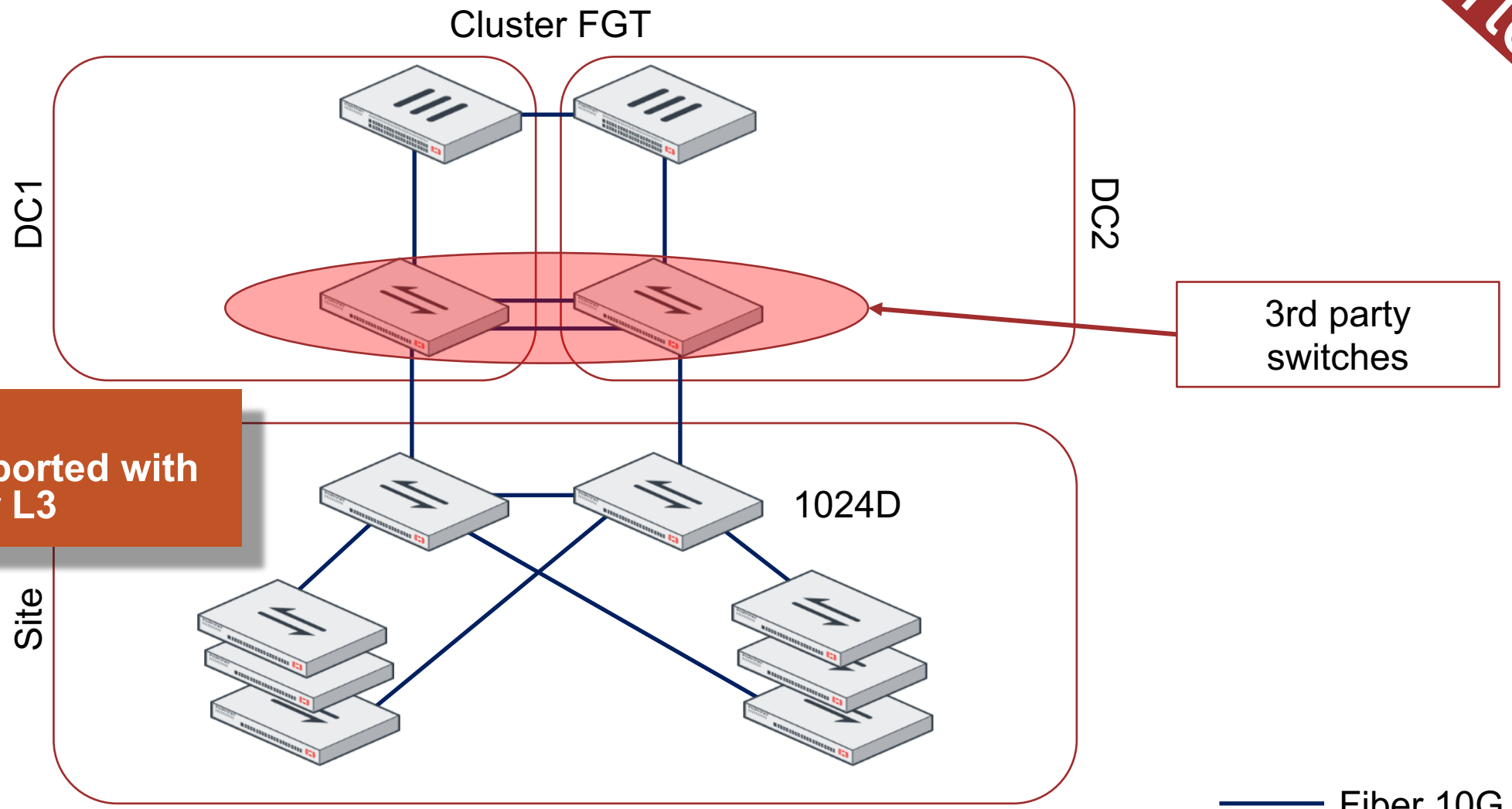
Supported



Design

Dual Home with – 3rd party switch between FGT and FSW

Not Supported



TIP

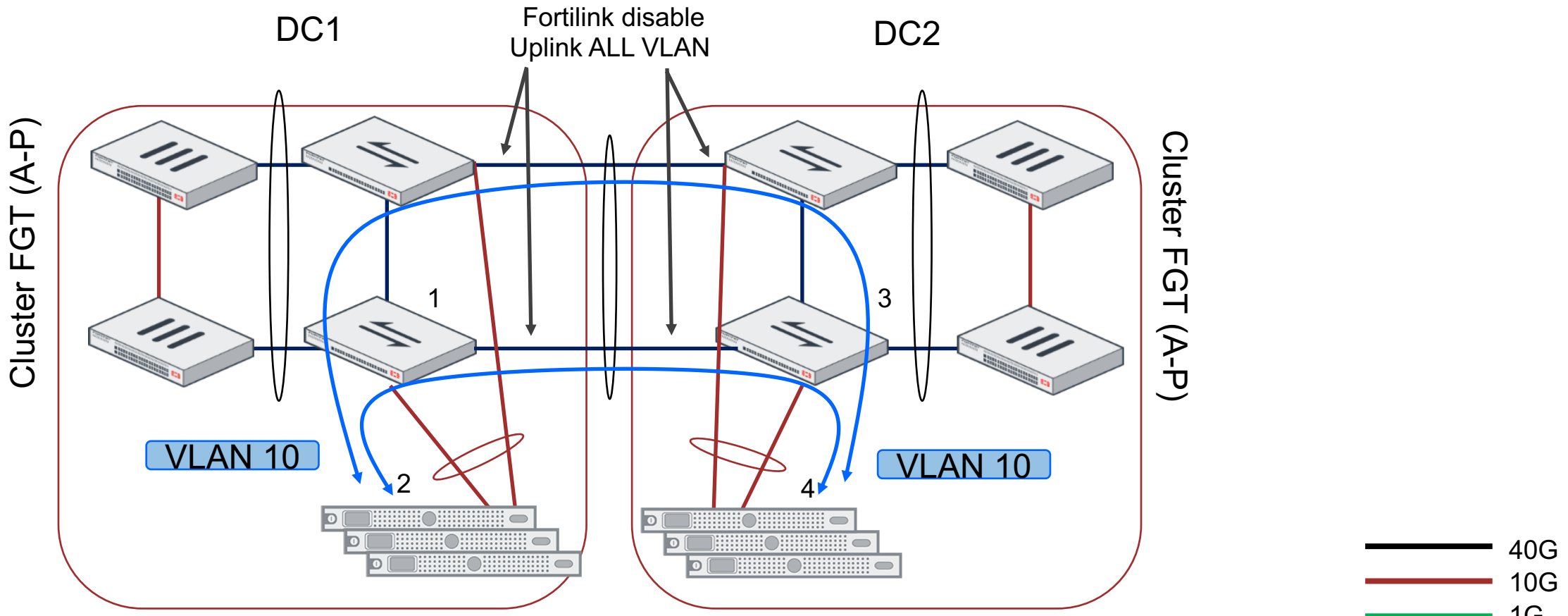
- **Could be supported with FortiLink over L3**

Design

Dual-Home (4 FGT / 2 cluster) & Distribution with 4 FSW

Supported

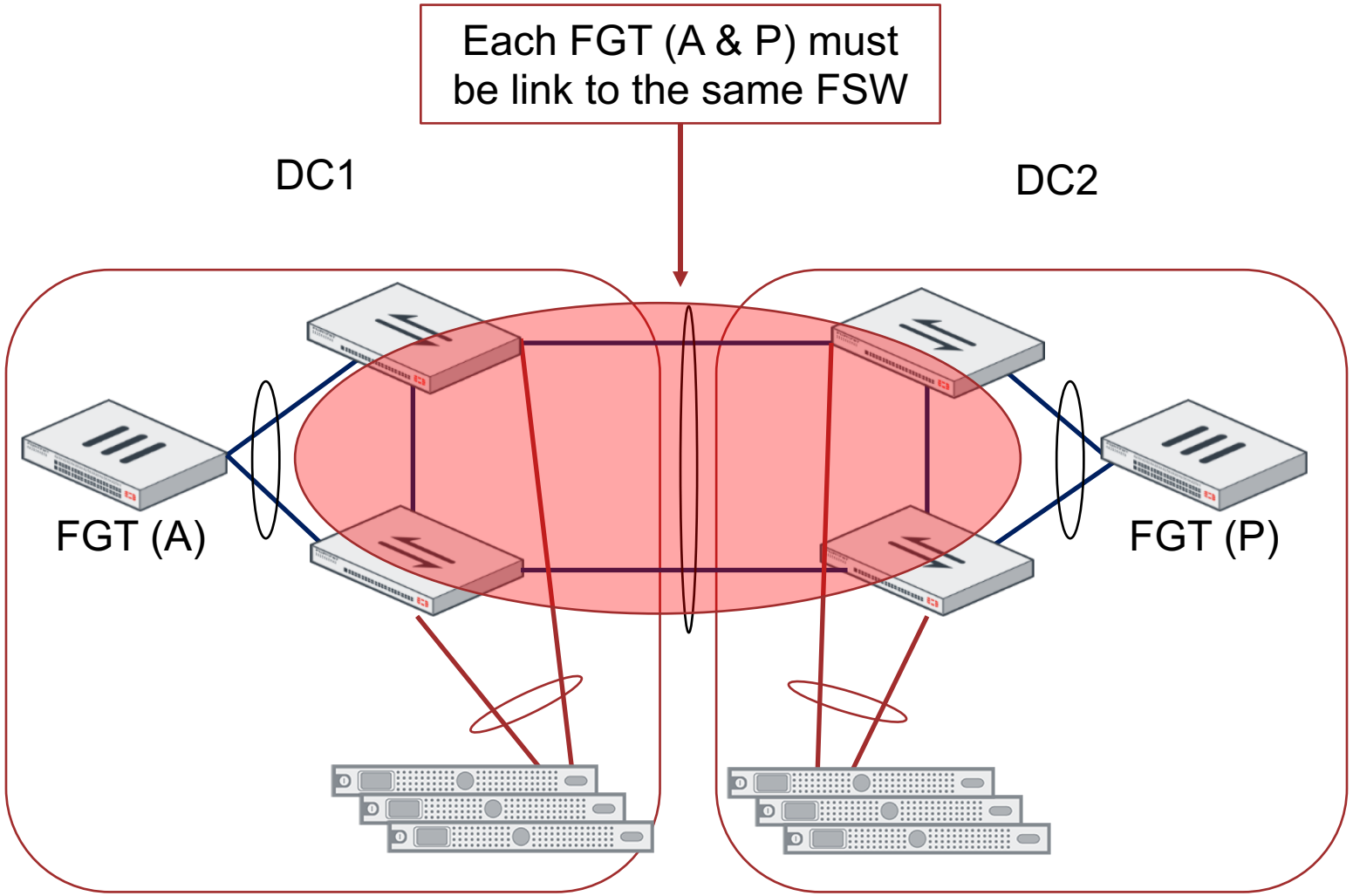
Each cluster on DC managed his 2 FortiSwitch, but L2 communication is possible between the two DC
VLAN ID is identical on both side but Interface VLAN is different between the two DC



Design

Dual-Home (2 FGT / 1 cluster) & Distribution with 4 FSW

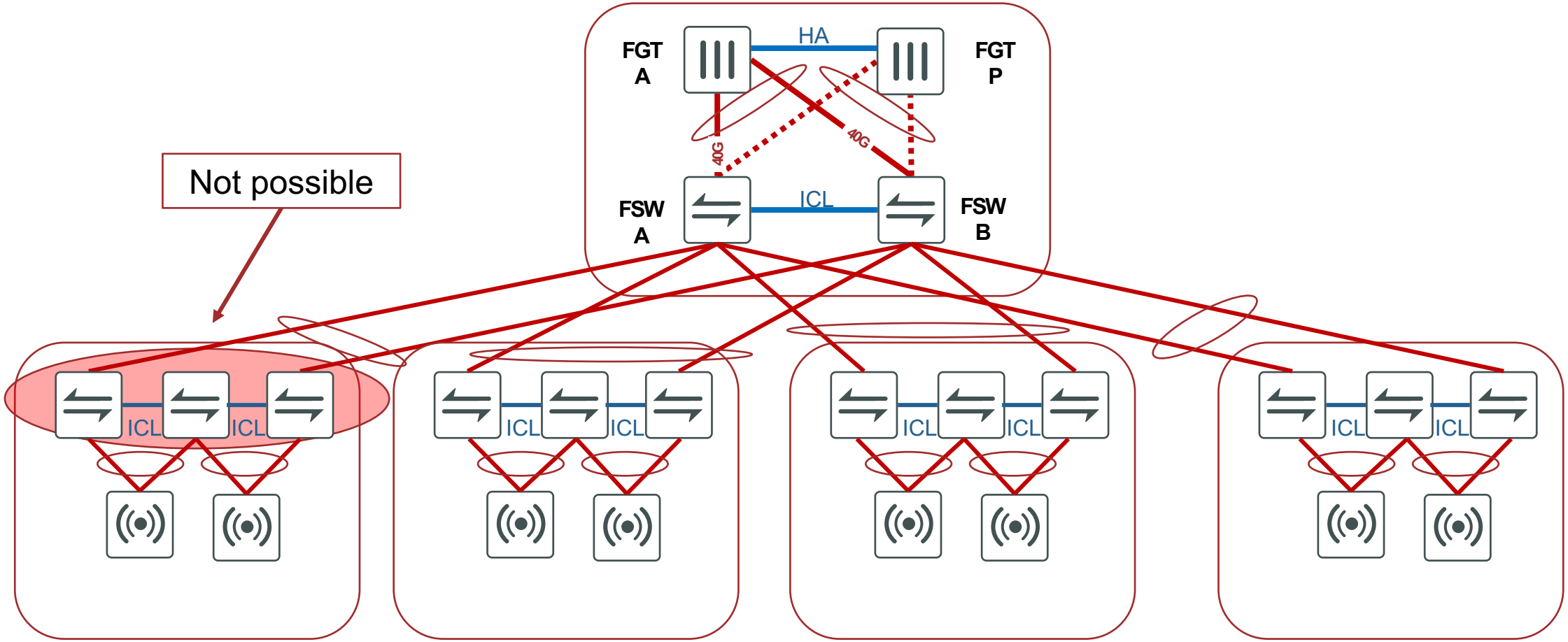
Not Supported

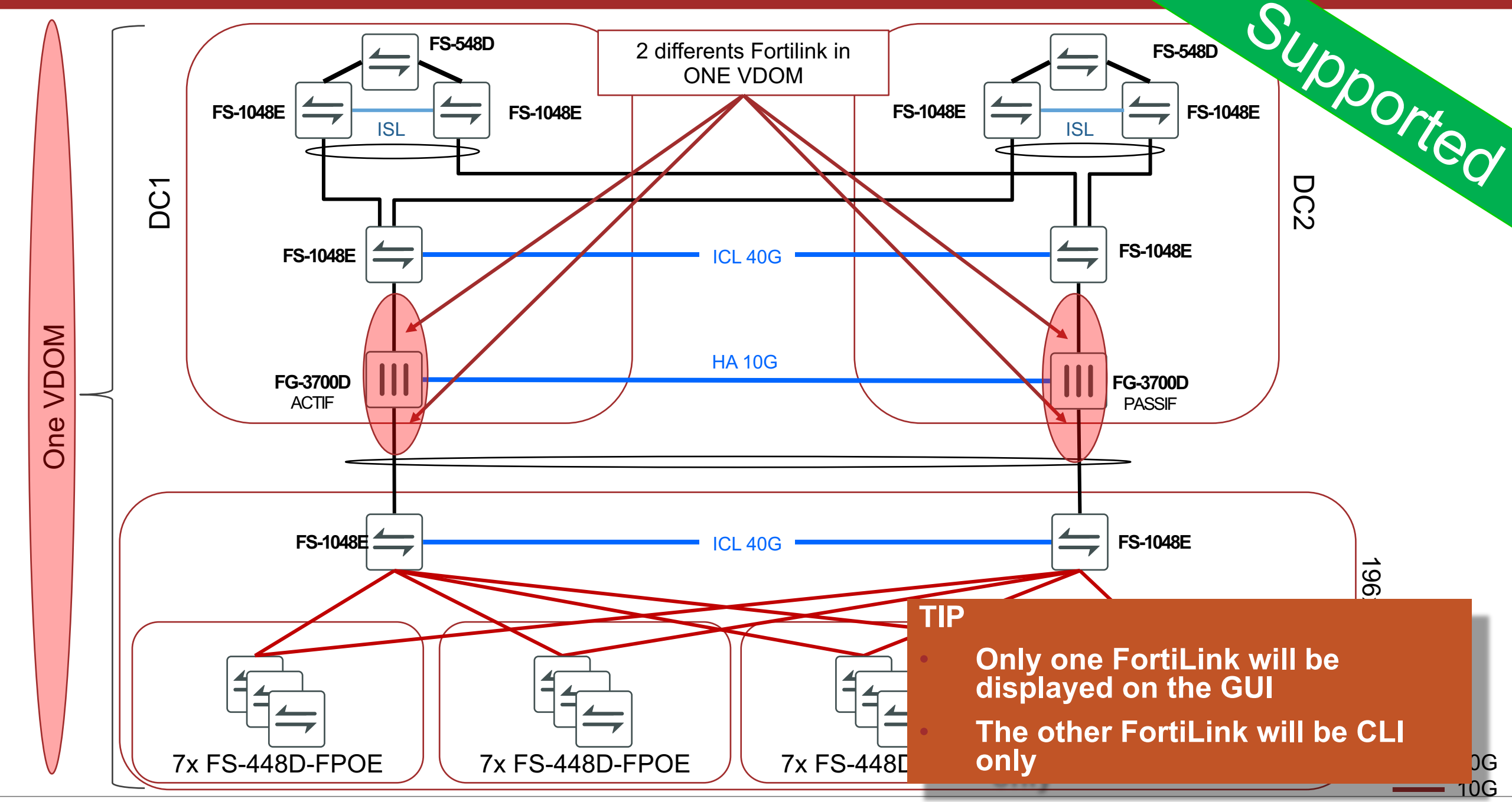


Design

Full MC-LAG – more than 2 FSW in MCLAG config

Not Supported

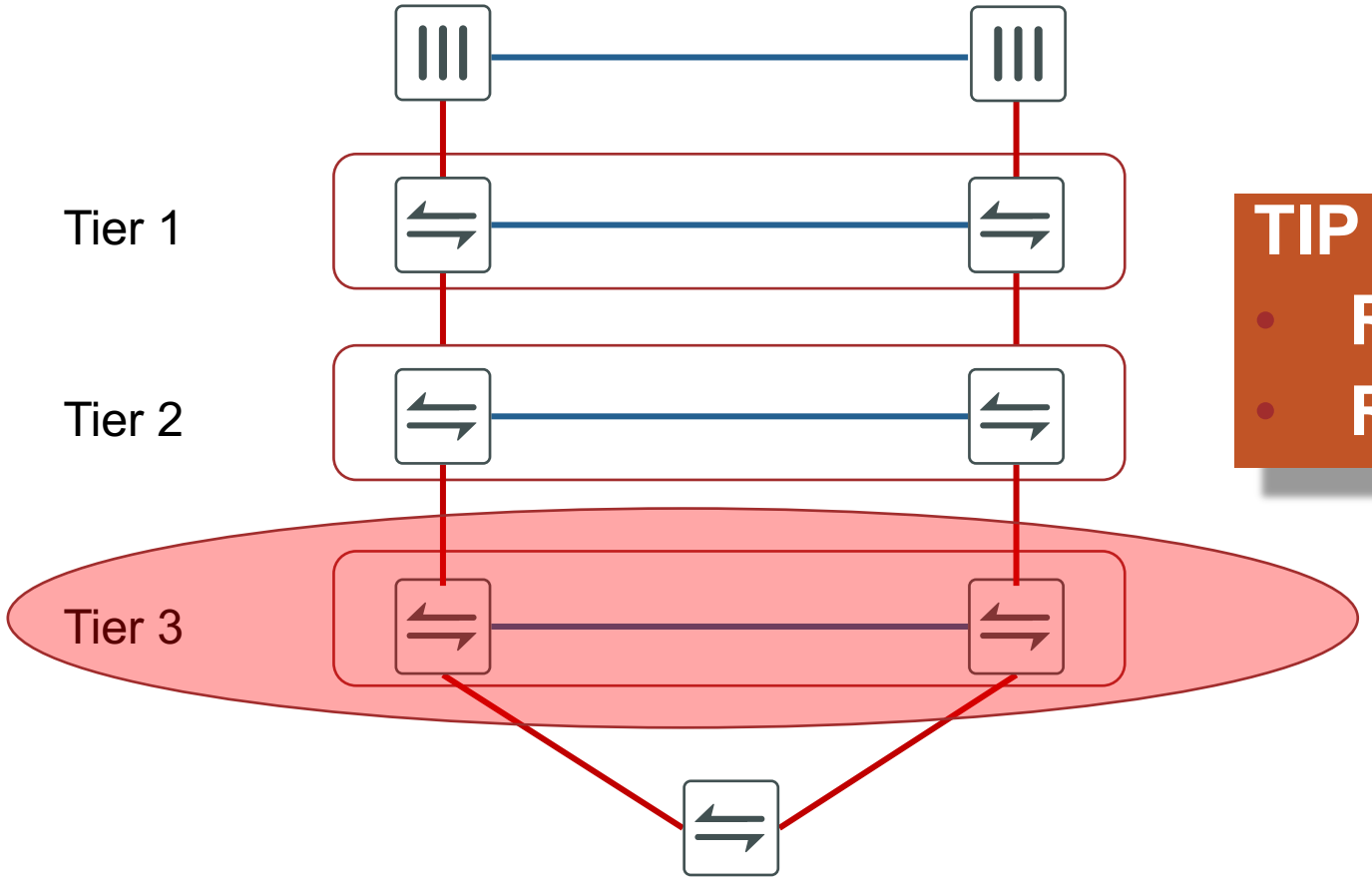



Supported
2 differents Fortilink in ONE VDOM
One VDOM
DC1
DC2
FS-548D
FS-1048E
ISL
FS-1048E
FS-548D
FS-1048E
ISL
FS-1048E
FS-1048E
ICL 40G
FS-1048E
FG-3700D
ACTIF
HA 10G
FG-3700D
PASSIF
FS-1048E
ICL 40G
FS-1048E
7x FS-448D-FPOE
7x FS-448D-FPOE
7x FS-448D
TIP
Only one FortiLink will be displayed on the GUI
The other FortiLink will be CLI only
10G

Design

MC-LAG – more than 2 MCLAG tiers

Not Supported



TIP

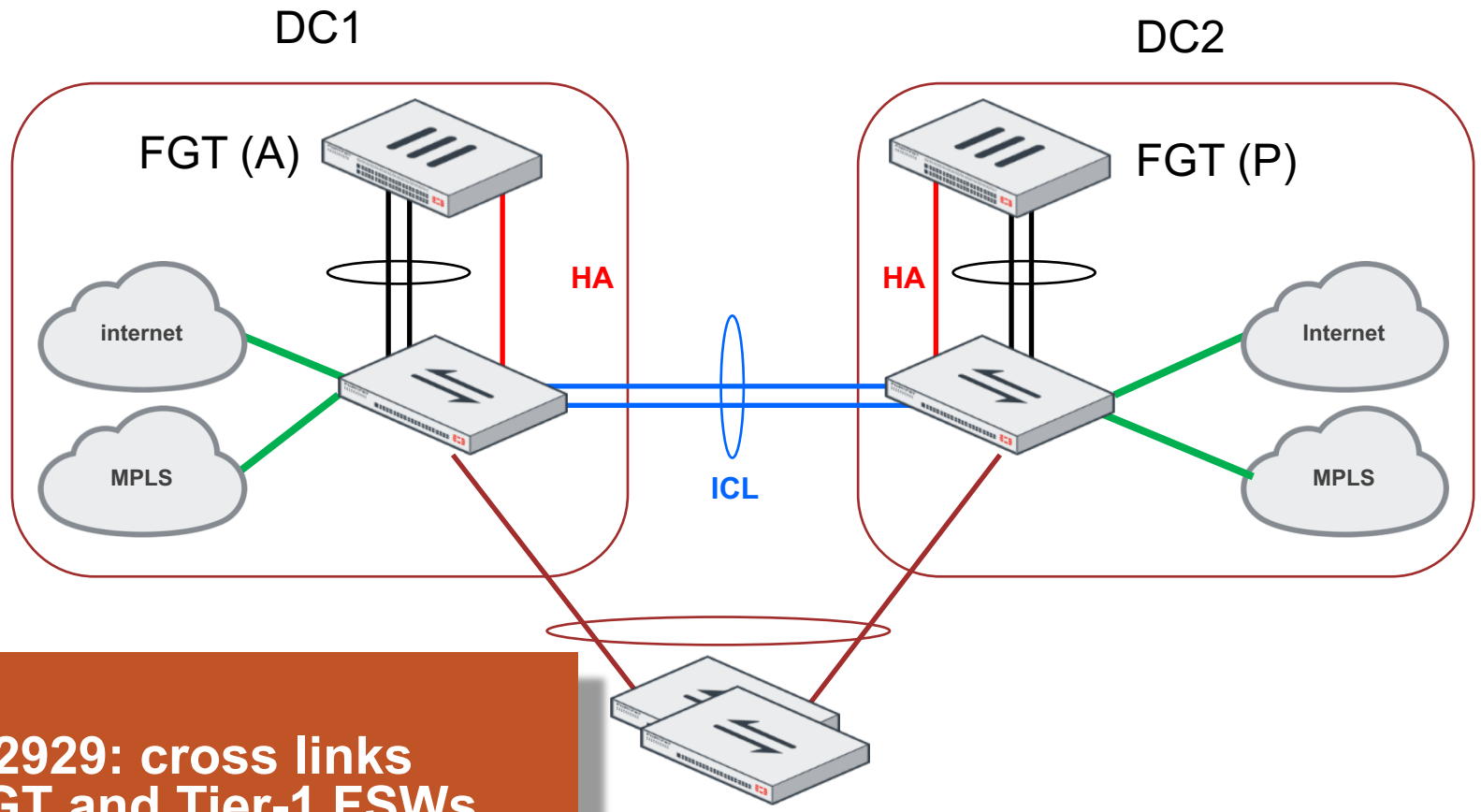
- **Requested to PM**
- **Requires TOP-3**

Design

Dual-Home (2 FGT / 1 cluster) & Distribution with 2 FSW & HA

Supported

http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverHeartbeat.htm



TIP

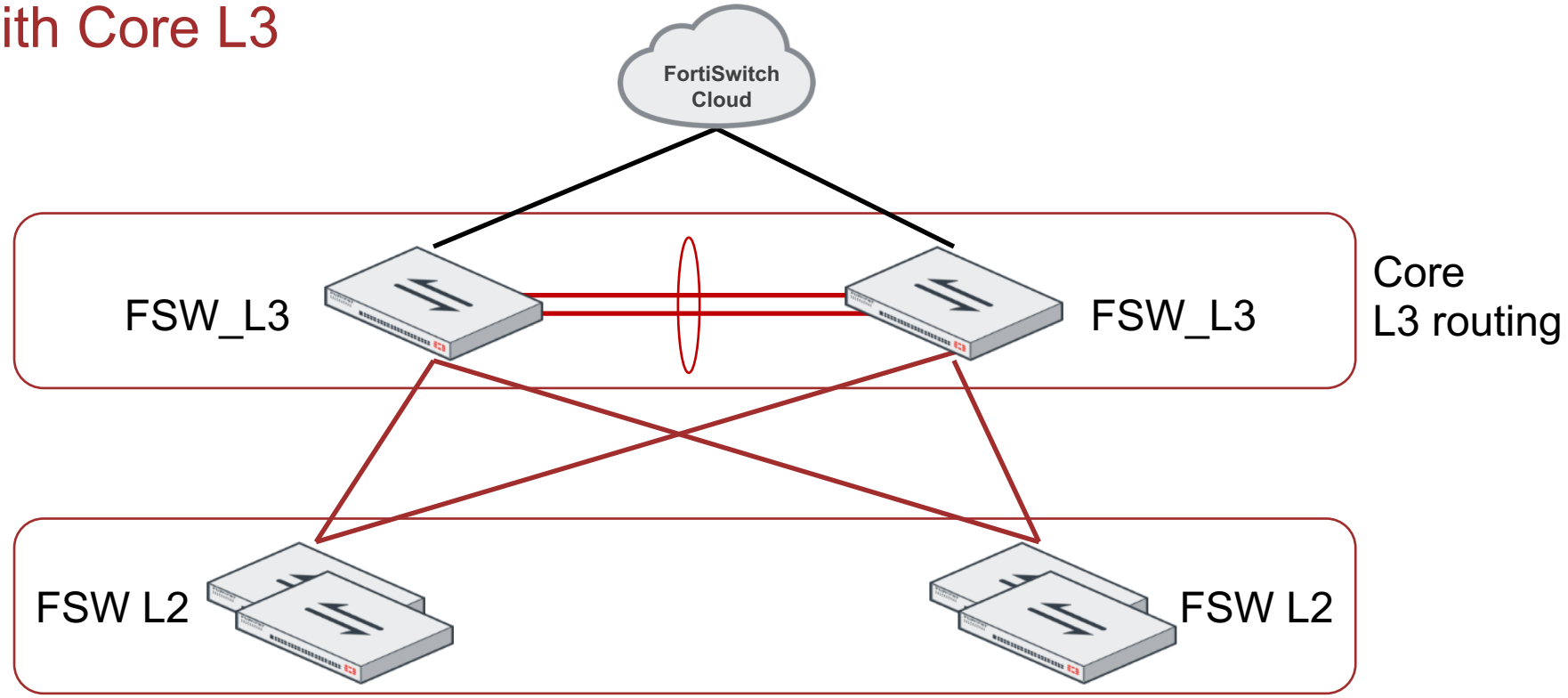
Mantis 0512929: cross links between FGT and Tier-1 FSWs

40G
10G
1G

Design

Cloud with Core L3

Supported



TIP

- **Each switch needs its own IP and internet connectivity.**
- **All the routing configuration must be done in CLI for now. ICL must be enabled in CLI as well**

40G
10G
1G

Live Demo

MC-LAG Setup

Quarantine

FortiCH-Office

Fortinet Switzerland